(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－215586
（P2002－215586A）
(43)公開日　平成14年８月２日(2002.8.2)

(51)Int.Cl.'		識別記号	FI		テーマコード'(参考)
G06F	15/00	330	G06F	15/00	330C　5B017
	12/14	320		12/14	320C　5B085
H04L	9/32		H04L	9/00	673A　5J104
					673B

審査請求　未請求　請求項の数20　ＯＬ　（全 25 頁）

(21)出願番号　特願2001－8311(P2001－8311)

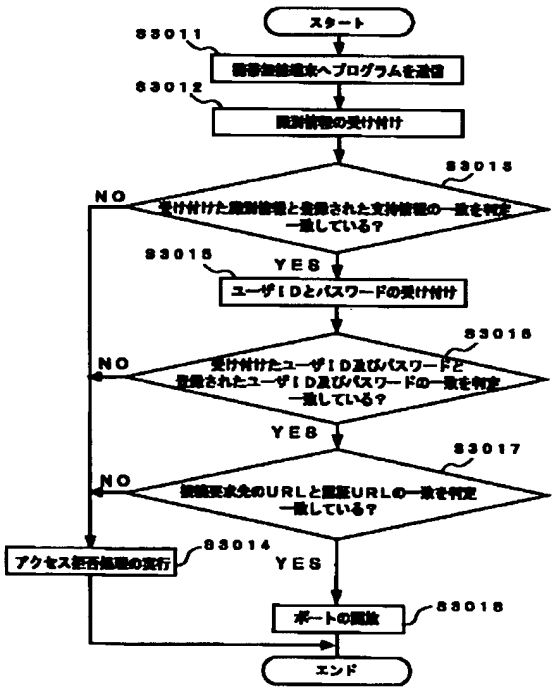
(22)出願日　平成13年１月16日(2001.1.16)

(71)出願人　000002107
住友重機械工業株式会社
東京都品川区北品川五丁目９番11号
(72)発明者　山元　達好
東京都品川区北品川五丁目９番11号　住友重機械工業株式会社内
(72)発明者　宮牧　秀宇
東京都品川区北品川五丁目９番11号　住友重機械工業株式会社内
(74)代理人　100099324
弁理士　鈴木　正剛　（外２名）

最終頁に続く

(54)【発明の名称】　認証装置及び方法、ネットワークシステム、記録媒体、コンピュータプログラム

(57)【要約】
【課題】　情報アクセスの際に、なりすましを行いにくい認証装置を提供する。
【解決手段】　携帯電話からアクセス要求があった場合、認証サーバは、当該携帯電話へ、プログラムを送信する（Ｓ３０１１）。このプログラムは、携帯電話のＲＯＭに改竄不能に記録された個体番号（例えば製造番号）についてのデータを読み出して、これを認証サーバへ送信させるためのものである。このプログラムの起動によって送信された製造番号についてのデータを受け付けた（Ｓ３０１２）認証サーバは、その製造番号を自らが保持している各携帯電話の製造番号についてのデータと比較し（Ｓ３０１３）、その製造番号が、保持していた製造番号のいずれかと一致する場合（Ｓ３０１３：Ｙｅｓ）には、そのアクセスが正当であるものと認証する。



1

【特許請求の範囲】

【請求項1】　所定の情報にアクセスしようとするユーザ端末が正当なものであるか否かの認証を行う装置であって、

ユーザ端末がアクセス可能な情報の範囲を示す範囲情報毎に割り当てられた許可情報と、認証対象となる複数のユーザ端末のそれぞれが有する改竄不能で且つ各ユーザ端末に固有の識別情報とを含む認証用情報が記録されている情報記録手段と、

認証を求めたユーザ端末からそのユーザ端末の認証用情報を受け付け、受け付けた認証用情報が前記情報記録手段に記録されている認証用情報のいずれかと一致する場合に当該ユーザ端末が正当なものであると判定する認証手段と、

前記認証を求めたユーザ端末が正当なものである場合に当該ユーザ端末による前記アクセスを許可する許可手段と、

を備えている、認証装置。

【請求項2】　前記範囲情報が、予めユーザ端末毎に登録したアクセス先のアドレスを含むものである、

請求項1記載の認証装置。

【請求項3】　前記許可情報がＩＤ及びパスワードの組からなるものであり、一つの前記識別情報について１組又は複数組のＩＤ及びパスワードが対応付けられている、

請求項1又は2記載の認証装置。

【請求項4】　一つの前記識別情報について１組のＩＤ及びパスワードが対応づけられており、該１組のＩＤ及びパスワードは前記アクセス先が複数の場合の統括的なＩＤ及びパスワードとして割り当てられている、

請求項1又は2記載の認証装置。

【請求項5】　前記統括的なＩＤ及びパスワードの使用を一括して停止又は停止解除させる手段をさらに備えている、

請求項4記載の認証装置。

【請求項6】　認証対象となるユーザ端末に対して各々の前記識別情報を当該ユーザ端末の操作者に知り得ない形態で送信させるためのプログラムを保持する手段と、認証を求めたユーザ端末に対して前記プログラムを送信する手段とを更に備えている、

請求項1記載の認証装置。

【請求項7】　前記プログラムは前記認証を求めたユーザ端末が前記識別情報を送信した後に消滅するものである、

請求項6記載の認証装置。

【請求項8】　前記ユーザ端末が携帯無線端末である、

請求項1ないし7のいずれかの項記載の認証装置。

【請求項9】　前記識別情報が、当該ユーザ端末の製造時に付与される個体番号である、

請求項1ないし7のいずれかの項記載の認証装置。

2

【請求項10】　前記ユーザ端末がアクセスしようとする前記情報が、セキュリティ性が要求される所定のネットワークの中に存在し、且つ、前記ネットワークの外に存するファイルと少なくともその一部が共通の内容に維持されている共通ファイルの記録情報である、

請求項1ないし9のいずれかの項記載の、認証装置。

【請求項11】　ユーザ端末がアクセス可能な情報を記録した第１サーバと、この第１サーバに記録されている前記情報にアクセスしようとするユーザ端末が正当なものか否かの認証を行う認証装置とを有し、

前記第１サーバは、正当と判定されたユーザ端末からのアクセスに呼応して該当情報を索出し、索出した情報を当該アクセスの発信元であるユーザ端末に送出するように構成されており、

前記認証装置は、

ユーザ端末がアクセス可能な情報の範囲を示す範囲情報毎に割り当てられた許可情報と、認証対象となる複数のユーザ端末のそれぞれが有する改竄不能で且つ各ユーザ端末に固有の識別情報とを含む認証用情報が記録されている情報記録手段と、

認証を求めたユーザ端末からそのユーザ端末の認証用情報を受け付け、受け付けた認証用情報が前記情報記録手段に記録されている認証用情報のいずれかと一致する場合に当該ユーザ端末が正当なものであると判定する認証手段と、

前記認証を求めたユーザ端末が正当なものである場合に当該ユーザ端末による前記アクセスを許可する許可手段と、

を備えている、ネットワークシステム。

【請求項12】　前記第１サーバがネットワークの中で、そのネットワークの外に存する第２サーバと専用線又は仮想専用線で接続されており、

前記第１サーバと前記第２サーバは、それぞれその記録情報の少なくとも一部が互いに共通の内容に維持される共通ファイルを保有するものであり、

前記認証装置は、前記第１サーバの共通ファイルの記録情報にアクセスしようとするユーザ端末が正当なものであるか否かの認証を行うものである、

請求項11記載のネットワークシステム。

【請求項13】　前記第１サーバ及び前記第２サーバの各々が、自己の共通ファイルの記録情報に変更が生じたときは変更前後の差分データを他方のサーバに送付するとともに、他方のサーバから前記差分データを受領したときは当該差分データを自己の共通ファイルに複写する複写タスクを自動実行するように構成されている、

請求項12記載のネットワークシステム。

【請求項14】　前記第１サーバが複数であり、前記第２サーバは複数の第１サーバのそれぞれに対応して設けられている、

請求項12記載のネットワークシステム。

【請求項１５】　前記認証装置が、前記第１サーバから前記ユーザ端末に送出された情報を抽出する抽出手段と、いかなる情報が送出されたかという送出情報についてのデータを各ユーザ端末毎に記録する送出情報記録手段と、を更に備えている、
請求項１１記載のネットワークシステム。
【請求項１６】　前記認証装置が、前記送出情報記録手段に記録された前記データに基づいて、そのユーザ端末についての送出情報を、当該ユーザ端末のディスプレイに表示するためのデータを生成する送出情報提示手段と、を更に備えている、
請求項１１記載のネットワークシステム。
【請求項１７】　ユーザ端末がアクセス可能な情報を記録した第１サーバを所定のネットワークの中で通信可能にする手段と、前記ネットワークを通じて前記情報にアクセスしようとするユーザ端末が正当なものであるか否かの認証を行う認証装置とを有し、
前記第１サーバは、正当なユーザ端末からのアクセスに呼応して該当情報を索出し、索出した情報を前記ネットワークを介して当該アクセスの発信元であるユーザ端末に送出するように構成されており、
前記認証装置は、ユーザ端末がアクセス可能な情報の範囲を示す範囲情報毎に割り当てられた許可情報と、認証対象となる複数のユーザ端末のそれぞれが有する改竄不能で且つ各ユーザ端末に固有の識別情報とを含む認証用情報が記録されている情報記録手段と、
認証を求めたユーザ端末からそのユーザ端末の認証用情報を受け付け、受け付けた認証用情報が前記情報記録手段に記録されている認証用情報のいずれかと一致する場合に前記ネットワークを介して行われる当該ユーザ端末が正当なものであると判定する認証手段と、
前記認証を求めたユーザ端末が正当なものである場合に当該ユーザ端末による前記アクセスを許可する許可手段と、
を備えている、ネットワークシステム。
【請求項１８】　前記第１サーバと前記ネットワークの外に存する第２サーバとを専用線又は仮想専用線で接続する手段と、前記第１サーバと前記第２サーバとが保有するファイルの少なくとも一部の記録情報を、互いに共通の内容に維持される共通ファイルにする手段とをさらに備え、
前記認証装置は、前記共通ファイルの記録情報にアクセスしようとするユーザ端末が正当なものであるか否かの認証を行うように構成されている、
請求項１７記載のネットワークシステム。
【請求項１９】　所定のネットワークの中にユーザ端末がアクセス可能な情報を記録した第１サーバが存するネットワークシステムに、前記情報にアクセスしようとするユーザ端末が正当なものであるか否かの認証を行う認証装置を配し、

該認証装置で、ユーザ端末がアクセス可能な情報の範囲を示す範囲情報毎に割り当てられた許可情報と、認証対象となる複数のユーザ端末のそれぞれが有する改竄不能で且つ各ユーザ端末に固有の識別情報とを含む認証用情報を記録しておき、
認証を求めたユーザ端末から少なくともそのユーザ端末の認証用情報を受け付け、受け付けた認証用情報が記録されている認証用情報のいずれかと一致する場合に当該ユーザ端末が正当なものであると判定し、
前記認証を求めたユーザ端末が正当なものである場合に当該ユーザ端末による前記アクセスを許可することを特徴とする、
ネットワークシステムにおけるユーザ端末の認証方法。
【請求項２０】　所定のネットワークの中にユーザ端末がアクセス可能な情報を記録した第１サーバが存し、前記第１サーバが、正当なユーザ端末からの求めに応じて該当情報を索出し、索出した情報を当該ユーザ端末に送出するネットワークシステムに配備されるコンピュータに、下記の処理を実行させるためのコンピュータプログラム。
（１）ユーザ端末がアクセス可能な情報の範囲を示す範囲情報毎に割り当てられた許可情報と、認証対象となる複数のユーザ端末のそれぞれが有する改竄不能で且つ各ユーザ端末に固有の識別情報とを含む認証用情報を記録する処理、（２）認証を求めたユーザ端末からそのユーザ端末の認証用情報を受け付け、受け付けた認証用情報が、記録されている認証用情報のいずれかと一致する場合に当該ユーザ端末が正当なものであると判定する処理、（３）前記認証を求めたユーザ端末が正当なものである場合に当該ユーザ端末による前記アクセスを許可する処理。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、例えば、携帯無線端末その他のユーザ端末を使用して情報提供等のサービスを行う際に使用される認証技術に関する。
【０００２】有線／無線通信手段を用いてインターネットに適宜接続可能なＰＤＡ（Personal Digital Assistants）やノートパソコン等のユーザ端末、インターネット接続機能やメール機能を有する携帯電話が普及している。これらのユーザ端末や携帯電話をインターネットメールサービスの端末として用いるなどして、サーバ側から個人ユーザ向けのサービスを提供したり、企業の業務に積極的に活用することが一般的になってきている。
【０００３】このようなサービスは、サーバ側で、ユーザ端末との間の通信とそれに伴う特定のサーバへのアクセスを制御することにより実現される。ユーザ端末等を用いたこの種のサービスは、通常、サービスの提供者が管理する特定の者（予め登録した者等）に対してのみ提供される。このような観点から、上述のようなサービス

を実行する場合は、サービスの提供を要求する者が、サービス提供者の管理下にある者であるか否かを確認するという認証の手続が必要となる。

【0004】認証は、何らかの許可情報、例えばユーザ名その他のユーザＩＤやパスワード等を用いて行われるのが一般的である。つまり、ユーザ端末からユーザが送ったユーザＩＤ及びパスワードと、サービス提供者が管理しているユーザＩＤ及びパスワードとを照合し、それが一致すれば当該ユーザは正当な者であり、一致しなければ当該ユーザは正当な者でないと判断し、正当な者であると判断されたユーザのみが所定のサービスを享受できるようにしている。

【0005】しかしながら、このような認証方法にも不具合がないわけではない。それは、ユーザＩＤ及びパスワードは、それが他人に盗まれた場合には、当該他人がそれを用いることで正規のユーザになりすますことが可能であるという点である。

【0006】

【発明が解決しようとする課題】本発明は、従来の認証技術を用いても防ぐことができなかった上記の「なりすまし」の問題を防ぐことができる新たな認証技術を提供することを、その課題とする。本発明は、また、かかる認証技術の応用技術を提供することを、その課題とする。

【0007】

【発明を解決するための手段】「なりすまし」の発生は、従来、認証に用いられていた許可情報は、それを入手さえできれば、ユーザ端末の如何を問わずに使用可能であることに起因する。これとは逆に、そのユーザ端末に固有の情報であって改竄不能な情報を認証に用い、その端末を用いた場合にしか正当なユーザによるアクセスだとの認証がなされないようにすれば、大半のなりすましを防止することができる。本発明は、このような知見に基づいてなされたものである。

【0008】本発明は、まず、所定の情報にアクセスしようとするユーザ端末が正当なものであるか否かの認証を行う装置であって、ユーザ端末がアクセス可能な情報の範囲を示す範囲情報毎に割り当てられた許可情報と、認証対象となる複数のユーザ端末のそれぞれが有する改竄不能で且つ各ユーザ端末に固有の識別情報とを含む認証用情報が記録されている情報記録手段と、認証を求めたユーザ端末からそのユーザ端末の認証用情報を受け付け、受け付けた認証用情報が前記情報記録手段に記録されている認証用情報のいずれかと一致する場合に当該ユーザ端末が正当なものであると判定する認証手段と、前記認証を求めたユーザ端末が正当なものである場合に当該ユーザ端末による前記アクセスを許可する許可手段とを備えている認証装置を提供する。この認証装置では、許可情報とユーザ端末自体に依存する識別情報とを含む認証用情報を用いて認証を行うので、許可情報の盗難とユーザ端末の盗難の双方がなされない限り、「なりすまし」が行えなくなり、認証の信頼性を高めることができる。範囲情報は、例えば、予めユーザ端末毎に登録したアクセス先のアドレスを含む情報である。この範囲情報によって、ユーザ端末がどの情報へアクセスする際に行う認証かがわかる。識別情報としては、例えば各ユーザ端末のＲＯＭ（Read Only Memory）に、製造時に記録される個体番号（例えば製造番号のようなもの）を用いることができる。なお、本明細書でいう「アクセス」は、情報の要求や取得のほか、ＦＡＸ指示や印刷指示のような各種指示を含む概念である。

【0009】許可情報としては、例えばＩＤ及びパスワードの組を用いることができる。この場合、一つの前記識別情報について１組又は複数組のＩＤ及びパスワードが対応付けられるようにする。一つの前記識別情報について１組のＩＤ及びパスワードを対応づけ、該１組のＩＤ及びパスワードは前記アクセス先が複数の場合の統括的なＩＤ及びパスワードとして割り当てられるようにしても良い。後者の場合は、前記統括的なＩＤ及びパスワードの使用を一括して停止又は停止解除させる手段をさらに備えるようにすることが好ましい。

【0010】認証対象となるユーザ端末に対して各々の前記識別情報を当該ユーザ端末の操作者に知り得ない形態で送信させるためのプログラムを保持する手段と、認証を求めたユーザ端末に対して前記プログラムを送信する手段とを更に備えて認証装置を構成しても良い。この場合、好ましくは、前記プログラムが前記認証を求めたユーザ端末が前記識別情報を送信した後に消滅するものとする。このようにすることで、何ら特別な機能を与えないユーザ端末からでも、認証装置への識別情報の送信を行えるようになる。

【0011】このようなプログラムとしては、例えばJava プログラムを用いることができ、その実行環境は、JVM(Java vertual Machine)、KVM（携帯電話等の携帯端末用のコンパクトなＪＶＭ）を使用することができる。このプログラムは、そのプログラムとユーザ端末が備える所定のハードウェアとの協働によって、識別情報の認証装置への送信を実現するようなものでも良く、そのプログラムとユーザ端末が備える所定のハードウェアとユーザ端末Ｔ１が有している所定のプログラムとの協働によって、識別情報の認証装置への送信を実現するようなものでも良い。

【0012】本発明におけるユーザ端末には、携帯無線端末を用いることができる。携帯無線端末は、例えば携帯電話、ＰＨＳ（Personal Handyphone System）、携帯電話やＰＨＳを利用したＰＤＡ（Personal Digital Assistants）又はノートパソコンなどが該当する。

【0013】上述の知見は、ネットワークシステムにも応用することができる。すなわち、本発明は、ユーザ端末がアクセス可能な情報を記録した第１サーバと、この

第1サーバに記録されている前記情報にアクセスしようとするユーザ端末が正当なものか否かの認証を行う認証装置とを有するネットワークシステムに適用が可能である。前記第1サーバは、正当と判定されたユーザ端末からのアクセスに呼応して該当情報を索出し、索出した情報を当該アクセスの発信元であるユーザ端末に送出するように構成されており、前記認証装置は、ユーザ端末がアクセス可能な情報の範囲を示す範囲情報毎に割り当てられた許可情報と、認証対象となる複数のユーザ端末のそれぞれが有する改竄不能で且つ各ユーザ端末に固有の識別情報とを含む認証用情報が記録されている情報記録手段と、認証を求めたユーザ端末からそのユーザ端末の認証用情報を受け付け、受け付けた認証用情報が前記情報記録手段に記録されている認証用情報のいずれかと一致する場合に当該ユーザ端末が正当なものであると判定する認証手段と、前記認証を求めたユーザ端末が正当なものである場合に当該ユーザ端末による前記アクセスを許可する許可手段とを備えているものである。

【0014】前記第1サーバが、ネットワークの中でそのネットワークの外に存する第2サーバ（第1サーバのものとその記録情報の少なくとも一部が互いに共通の内容に維持される共通ファイルを保有するサーバ）と専用線又は仮想専用線で接続されているものとすることもできる。この場合、前記認証装置は、前記第1サーバの通ファイルの記録情報にアクセスしようとするユーザ端末が正当なものであるか否かの認証を行うように構成する。第1サーバと第2サーバとが接続されるネットワークシステムの場合、これらのサーバの各々は、それぞれ自己の共通ファイルの記録情報に変更が生じたときは、変更前後の差分データを他方のサーバに送付するとともに、他方のサーバから前記差分データを受領したときは当該差分データを自己の共通ファイルに複写する複写タスクを自動実行するように構成する。第2サーバは複数の第1サーバのそれぞれに対応して設けられる構成も、本発明によれば可能である。

【0015】本発明のネットワークシステムに備えられる前記認証装置は、前記第1サーバから前記ユーザ端末に送出された情報を抽出する抽出手段と、いかなる情報が送出されたかという送出情報についてのデータを各ユーザ端末毎に記録する送出情報記録手段と、を更に備えるようにしても良い。あるいは、前記送出情報記録手段に記録された前記データに基づいて、そのユーザ端末についての送出情報を、当該ユーザ端末のディスプレイに表示するためのデータを生成する送出情報提示手段と、を更に備えるようにしても良い。このような認証装置であれば、一度ユーザが使用した情報についての送出情報を、見出しの如き状態で当該ユーザ端末に表示できるようになるため、ユーザにとって便宜である。

【0016】本発明は、第1サーバを事後的に接続できるようにしたネットワークに適用することもできる。このネットワークシステムは、ユーザ端末がアクセス可能な情報を記録した第1サーバを所定のネットワークの中で通信可能にする手段と、前記ネットワークを通じて前記情報にアクセスしようとするユーザ端末が正当なものであるか否かの認証を行う認証装置とを有するシステムである。第1サーバは、正当なユーザ端末からのアクセスに呼応して該当情報を索出し、索出した情報を前記ネットワークを介して当該アクセスの発信元であるユーザ端末に送出するように構成されている。また、認証装置は、ユーザ端末がアクセス可能な情報の範囲を示す範囲情報毎に割り当てられた許可情報と、認証対象となる複数のユーザ端末のそれぞれが有する改竄不能で且つ各ユーザ端末に固有の識別情報とを含む認証用情報が記録されている情報記録手段と、認証を求めたユーザ端末からそのユーザ端末の認証用情報を受け付け、受け付けた認証用情報が前記情報記録手段に記録されている認証用情報のいずれかと一致する場合に前記ネットワークを介して行われる当該ユーザ端末が正当なものであると判定する認証手段と、前記認証を求めたユーザ端末が正当なものである場合に当該ユーザ端末による前記アクセスを許可する許可手段とを備えているものである。

【0017】前者のネットワークシステム及び第1サーバが接続された後者のネットワークシステムは、ユーザ企業別のグループウェア（一般に、グループウェアの語は、共通の仕事や目的をもったグループが行う作業を支援するコンピュータソフトウェアを指すが、この特許明細書では、それを実現するためのハードウェア資源をも含む概念を意味する。）を実現する環境を容易に構築することができる。企業における業務の形態は多様化しており、一人で業務を収束させることは稀で、通常は、グループウェアを用いて複数の人間が協調して業務を遂行するようになっている。グループウェアは、例えば、ファイアウォールで保護されたイントラネットに、社員が操作する複数のユーザ端末（クライアント端末）とこのユーザ端末からのアクセスを一定条件下で受け付ける第1サーバとを接続し、第1サーバに、ユーザインタフェース機能やセキュリティ機能等を形成するためのコンピュータプログラムを搭載して実現される。通常、イントラネットには、インターネットプロバイダのWWW（World Wideウエブ）サーバも接続されており、電子メールに関しては、インターネットを媒介として外部端末からもイントラネット内で受け渡しできるようになっている。企業内のイントラネットに当該企業の社内情報を管理するサーバを設け、このサーバに上記の各種端末を接続できる環境を構築できれば、当該企業の社員が任意の時点で任意の箇所から社内情報にアクセスすることが可能になり、企業の業務への活用形態としては、極めて好ましいものとなる。しかし、イントラネットを活用するためには、以下のような課題もある。

（1）インターネットメールサービスの利用を前提とし

た社内情報のアクセス形態では、守秘義務のない者が運営するWWWサーバが介在することになるため、セキュリティ性を十分に確保できるかどうかがわからない。

（2）セキュリティ性確保のために、例えばグループウェアを実現するための各種端末同士をすべて専用回線で接続したり、あるいは企業の本社のイントラネットと各支店のイントラネット及び本社及び各支店のイントラネット同士をすべて専用回線で結ぶことも考えられるが、そうすると必然的に多くの専用回線の敷設が必要となり、運用を維持する費用の飛躍的な増加を招くため、コスト高となる。

（3）既存のインターネットメールサービスを業務に使用しようとすると、携帯電話サービス事業者が標準的に提供するインターネットメールサービスでは、当該事業者の設定するサービス条件による、例えば、一件のメールの文字数、メールサーバに蓄積できるメールの件数、添付文書の形態等の制限があるため、大きなデータの送信が難しくなり、また、携帯電話の場合、その機種毎にメール機能の操作方法が少しずつ異なるため、操作に関する統一的な教育および習熟が困難となるので、グループウェアの操作性が良くない。

（4）携帯電話から通知を受けた企業スタッフが通知内容のアプリケーションプログラムを手動で起動させたり、有線通信による特定のサービス提供体において用意されているコンピュータが予め登録されたアプリケーションプログラムをディジタル有線端末から入力される制御信号の内容を解読して自動的に起動実行することは、従来より行われているが、上記のサービス提供体等による既存のインフラストラクチャ（infrastructure）を利用せずに、独自に用意したアプリケーションプログラムを携帯電話端末等から任意に起動実行させることは、現在のところ行われておらず、グループウェアの拡張性に問題が残る。このような課題を解決するのが上述の各ネットワークシステムである。

【0018】本発明は、また、所定のネットワークの中にユーザ端末がアクセス可能な情報を記録した第1サーバが存するネットワークシステムに、前記情報にアクセスしようとするユーザ端末が正当なものであるか否かの認証を行う認証装置を配し、該認証装置で、ユーザ端末がアクセス可能な情報の範囲を示す範囲情報毎に割り当てられた許可情報と、認証対象となる複数のユーザ端末のそれぞれが有する改竄不能で且つ各ユーザ端末に固有の識別情報とを含む認証用情報を記録しておき、認証を求めたユーザ端末から少なくともそのユーザ端末の認証用情報を受け付け、受け付けた認証用情報が記録されている認証用情報のいずれかと一致する場合に当該ユーザ端末が正当なものであると判定し、前記認証を求めたユーザ端末が正当なものである場合に当該ユーザ端末による前記アクセスを許可することを特徴とする、ネットワークシステムにおけるユーザ端末の認証方法を提供する。

【0019】本発明は、また、所定のネットワークの中にユーザ端末がアクセス可能な情報を記録した第1サーバが存し、前記第1サーバが、正当なユーザ端末からの求めに応じて該当情報を索出し、索出した情報を当該ユーザ端末に送出するネットワークシステムに配備されるコンピュータに、下記の処理を実行させるためのコンピュータプログラムを提供する。

（1）ユーザ端末がアクセス可能な情報の範囲を示す範囲情報毎に割り当てられた許可情報と、認証対象となる複数のユーザ端末のそれぞれが有する改竄不能で且つ各ユーザ端末に固有の識別情報とを含む認証用情報を記録する処理、

（2）認証を求めたユーザ端末からそのユーザ端末の認証用情報を受け付け、受け付けた認証用情報が、記録されている認証用情報のいずれかと一致する場合に当該ユーザ端末が正当なものであると判定する処理、

（3）前記認証を求めたユーザ端末が正当なものである場合に当該ユーザ端末による前記アクセスを許可する処理。

【0020】

【発明の実施の形態】次に、図面を参照して本発明の好適な実施の形態を説明する。

＜全体構成＞図1は、本発明が適用されるネットワークシステムの全体構成例を示した図である。本実施形態のネットワークシステムは、公衆通信網ＤＮが敷設された管理企業に設置されるセキュアなイントラネットＬＮを有する、事後的に構築可能なネットワークシステムである。イントラネットＬＮは、それぞれ専用回線網ＰＮと接続可能な複数のセグメントＳａ～Ｓｎを有している。セグメントＳａ～Ｓｎは、それぞれ管理の対象となるユーザ企業の第1サーバであるホストサーバ１０ａ，１０ｂ，・・・を配備するために割り当てられる。イントラネットＬＮの入口付近には、認証サーバ1、ファイアウォール（ＦＷ）１１及びルータ１２が設けてあり、正当なユーザ端末Ｔ１からの特定のアクセスのみが、これらを通過してイントラネットＬＮ内のいずれかのセグメントＳａ～Ｓｎに導かれるようになっている。つまり、イントラネットＬＮの外部からのアクセスに対するセキュリティ性が維持されている。

【0021】ファイアウォール１１には、ユーザ端末Ｔ１からのアクセスが、無線網ＷＮを含む携帯電話網ＭＮと、携帯電話網ＭＮ内のルータ１４を介して接続された公衆通信網ＤＮと、この公衆通信網ＤＮを介して接続されたルータ１２とを通じて導かれる。携帯電話網ＭＮは、携帯電話による通信サービス事業を提供する事業体が管理するものである。なお、ここでいう携帯電話には、狭義の携帯電話（携帯電話無線機）のほか、ＰＨＳも含むものとする。

【0022】ユーザ端末Ｔ１は、ノートパソコンやＰＤ

Aのようなユーザ端末と上記の携帯電話とを組み合わせたものである。インテリジェントな携帯電話（情報処理機構を有する携帯電話）の場合は、その携帯電話単体でユーザ端末となり得る。ユーザ端末Ｔ１には、ブラウザ画面を形成するためのブラウザプログラムが搭載される。このブラウザプログラムは、ユーザ端末Ｔ１に当初から搭載しておいても良く、「Ｊａｖａアプレット（Ｊａｖａは米国サン・マイクロシステムズの商標）」として、ホストサーバ１０の側からその都度送出するようにしても良い。

【００２３】ユーザ端末Ｔ１は、改竄不能で且つ各ユーザ端末に固有の情報である識別情報を有している。携帯電話には、通常、その製造番号その他の個体番号についての固有データを記録したＲＯＭ又はＳＩＭカード（又はその他のＩＤカード）が搭載されており、この固有データは、携帯電話の製造時に一度書き込まれたら書き換え不能となっている。本実施形態では、この固有データに基づく個体番号を上述の識別情報として利用する。ユーザ端末Ｔ１には、また、上述の識別情報を読み出して送出するためのプログラムが搭載されている。例えば、Ｊａｖａ以外の言語で既述されたプログラムが搭載されている。さらに、ユーザ端末Ｔ１には、Ｊａｖａの実行環境の一つであるＫＶＭを使用することで、上記の識別情報を、携帯電話の場合であれば、そのＲＯＭから読み出せるような環境が準備されている。ユーザ端末Ｔ１には、また、テンキーなどで構成される入力部が設けられており、ＩＤ（後述する認証ＩＤとユーザＩＤ）とパスワード（後述する認証パスワードとユーザパスワード）の入力を行えるようになっている。

【００２４】携帯電話網ＭＮには、良く知られているように、ＤＮＳ（Domain Name Server）３０が設けられており、インターネットＩＮにもグローバルなＤＮＳ４０が設けられている。ＤＮＳ３０及びＤＮＳ４０は、ドメイン名とＩＰ（InternetProtocol）アドレスとの対応関係を記述したアドレステーブルを有しており、それぞれ相互にアドレステーブルを参照することにより、アクセス時のアドレスの相違を解決できるようになっている。

【００２５】専用回線網ＰＮは、専用回線又は仮想専用回線（例えば暗号化技術及びカプセル技術を用いて公衆回線を仮想的に当事者間で専用化した回線（バーチャル・プライベート・ネットワーク））の集合からなる通信網である。専用回線網ＰＮとしては、いわゆる次世代通信網（例えば「ＰＲＩＳＭ（ＰＲＩＳＭは日本テレコム株式会社の登録商標）」と呼ばれる専用回線網）が実用化の域にあり、日本全国又は世界中に、複数のアクセスポイントが用意されているので、これを利用することで、運用コストを低減させることができる。本実施形態では、遠隔地に存するユーザ企業の第２サーバの一例となるローカルサーバ２０ａ，２０ｂを、それぞれ最寄りのアクセスポイントから専用回線網ＰＮに接続し、この専用回線網ＰＮを介して対応するホストサーバ１０ａ，１０ｂと双方向通信可能な形態で接続されるようにしておく。

【００２６】＜イントラネットの構成＞イントラネットＬＮの詳細な構成例を図２に示す。図２は、５つのセグメントＳａ～Ｓｅからなるイントラネットの例を示している。各セグメント、例えばセグメントＳａは、複数の接続ポートを有している。その一つは、ホストサーバ１０ａに接続されるものであり、他の一つはルータ１３に接続されるものである。ルータ１３のポートに専用回線網ＰＮの特定の回線を接続することにより、ユーザ企業が、個別的にセグメントＳａを使用することができるようになっている。なお、セグメントＳａと専用回線網ＰＮとの間にスイッチング・ハブ（インテリジェント型通信路切替装置）又はルータを設け、これを介して専用回線網ＰＮに接続するようにしても良い。他のセグメントＳｂ～Ｓｅについても同様となる。

【００２７】各セグメントＳａ～Ｓｅの接続ポートに、ホストサーバ１０ａ～１０ｅが配備され、各ホストサーバ１０ａ～１０ｅにスイッチング・ハブ１４及び専用回線網ＰＮを介してローカルサーバが接続された状態では、イントラネットＬＮ内にセキュアなハウジングが構築される。すなわち、すべてのホストサーバ１０ａ～１０ｅと対応するローカルサーバとは専用回線網ＰＮで接続されるから第三者が介入する余地がなく、各ホストサーバ１０ａ～１０ｅが配備されるセグメントＳａ～Ｓｅはそれぞれファイアウォール１１で保護されているから、不正アクセス者が侵入することが困難なハウジングとなる。従って、このようなハウジングの個々のセグメントＳａ～Ｓｅをユーザ企業用に割り当てることで、ユーザ企業にとっては、安価なコストでセキュアな自社専用のネットワーク環境（又はグループウェア環境）を構築できるようになる。

【００２８】＜ルータの構成＞ルータ１２，１３，１４は、ＯＳＩ（Open Systems Interconnection）基本参照モデルの第３層（ネットワーク層）でルーティング（経路制御）を行う。ネットワーク層で接続されるため、ＯＳＩ基本参照モデルの第２層（データリンク層）以下が異なっていてもデータの中継が可能である。経路設定機能も持ちあわせているので、例えばイントラネットＬＮと公衆通信網ＤＮ、イントラネットＬＮと専用回線網ＰＮのような異なるネットワークの接続も可能である。

【００２９】図３は、ルータの構成例を示した図である。ルータは、双方向のルーティングを行うため、伝送路Ｒ１，Ｒ２に対して、受信レシーバＲＲ及び受信バッファＲＢと、送信ドライバＳＤ及び送信バッファＳＢとを対照に設け、さらに、ルーティング実行部Ｕ１、ＮＡＴ（Network Address Translation）テーブルＮＴ、ＲＩＰ（Routing Information Protocol）実行部Ｕ２を具備している。受信レシーバＲＲは、伝送路Ｒ１，Ｒ２か

らデータを受信するものである。受信バッファＲＢは、受信したデータを蓄積するものである。送信ドライバＳＤは、伝送路Ｒ１，Ｒ２へデータを送信（転送）するものである。送信バッファＳＢは、送信（転送）すべきデータを蓄積するものである。ルーティング実行部Ｕ１は、受信したＲＩＰを処理してアドレス変換を行い、通信路を確立するものである。ＲＩＰ実行部Ｕ２は、必要なＲＩＰを伝送路Ｒ１，Ｒ２に送出するものである。ＮＡＴテーブルＮＴには、アドレス変換の際に使用されるアドレス、すなわち宛先のアドレスを表す「Destination」と、着信元のアドレスを表す「Source」が記録されている。

【００３０】図４は、イントラネットＬＮの外側のルータ１２が具備するＮＡＴテーブルの内容例を示した図である。図４（ａ）は公衆通信網ＤＮからファイアウォール１１に向かうデータをルーティングする場合のＮＡＴテーブル、図４（ｂ）はファイアウォール１１から公衆通信網ＤＮに向かうデータをルーティングする場合のＮＡＴテーブルの例を示している。「2××.111.22.33」はドメイン登録されたユーザ企業のローカルサーバ２０のＩＰアドレス、「1××.111.22.33」はホストサーバ１０のＩＰアドレス、「2××.444.55.6」は発信端末のインターネットにおけるＩＰアドレス、「1××.444.55.6」はイントラネットＬＮで認識可能な発信端末のＩＰアドレスである。ＮＡＴテーブルを図４のように設定することで、インターネットとは異なるＩＰアドレスでイントラネットＬＮにアクセスできるようになる。

【００３１】ルータ１３には、ファイアウォール１１を通過したアクセスの発信端末のアドレスと、管理対象となるホストサーバのアドレスとをＮＡＴテーブルに設定しておく。ＮＡＴテーブルをこのように設定することにより、ファイアウォール１１を通過したアクセスの発信端末とセグメント（それに配備されるホストサーバ）との間に、選択的に通信路を確立する通信路制御手段を実現することができる。スイッチングハブ１４に代えて、ルータを用いる場合も同様の手順でアドレスをＮＡＴテーブルに設定することになる。

【００３２】＜ホストサーバとローカルサーバ＞ホストサーバ（図1の１０ａ，１０ｂ、図2の１０ａ～１０ｅ、以下、個々のものを識別する必要がない場合はサフィックスを省略した符号１０で表す）及びローカルサーバ（図1の２０ａ，２０ｂ以下、個々のものを識別する必要がない場合はサフィックスを省略した符号２０で表す）について説明する。原則として、一つのホストサーバ１０に一つのローカルサーバ２０が対応し、それぞれ専用回線網ＰＮを介して接続されるようになっている。但し、一つのホストサーバ１０に複数のローカルサーバ２０が対応していても良く、個々のローカルサーバ２０に１又は複数のクライアント端末が接続される独自のＬＡＮ（Local Area Network）が接続されていても良い。要は、イントラネットＬＮの中に存するホストサーバ１０とイントラネットＬＮの外に存するローカルサーバ２０とが1対1に対応していれば足りる。

【００３３】ホストサーバ１０は、データ転送可能なウエブメールサーバ機能、検索機能、複写機能、スケジューラ機能を有し、さらに、ユーザがアクセスしようとする情報であるメールファイルやスケジュールファイル等を含むデータベースを具備するコンピュータである。検索機能はデータベースの該当ファイルを検索する機能であり、複写機能はローカルサーバ２０との間でデータベースの変更分のデータの複写を行う複写タスクを起動実行する機能である。スケジュール機能は、登録したユーザ企業毎に用意されているスケジュールファイルを管理する機能である。ローカルサーバ２０は、少なくとも上記の複写機能とデータベースとを有するコンピュータである。

【００３４】必ずしもその必要はないが、この実施形態では、ホストサーバ１０とローカルサーバ２０の各々が具備するデータベース内のファイルの少なくとも一部は、他方のサーバのものと共通の内容に維持される共通ファイルとされる。ホストサーバ１０とローカルサーバ２０とでグループウェアを構成している場合は、当該グループウェア内で共通内容となる共通ファイルとされる。例えば、ローカルサーバ２０内のメールファイルやスケジュールファイルの内容がそのままホストサーバ１０内のメールファイルやスケジュールファイルの内容となる。従って、ホストサーバ１０の共通ファイルにアクセスすれば、それは、ローカルサーバ２０で管理している共通ファイルにアクセスしたのと、実質的に等価となる。

【００３５】ホストサーバ１０とローカルサーバ２０の共通ファイルの内容を共通に維持するための形態には種々考えられるが、この実施形態では、各サーバで互いに複写タスクを実行することで、これを実現する。すなわち、ローカルサーバ２０が自己の共通ファイルに変更が生じたときに変更前後の差分データをホストサーバ１０に送付するとともに、ホストサーバ１０から差分データを受領したときは、当該差分データを自己の共通ファイルに複写する。ホストサーバ１０の共通ファイルに変更が生じた場合の複写タスクも同様に行われる。

【００３６】＜認証サーバの構成＞次に、認証サーバ1について説明する。認証サーバ１は、本発明における認証装置に相当するもので、ユーザ端末Ｔ１からホストサーバ１０の共通ファイルに記録された情報へのアクセス要求があった場合に、そのユーザ端末Ｔ１が正当なものであるか否かの認証を行い、正当なものであるときに当該ユーザ端末Ｔ１による上記アクセスを許可するものである。

【００３７】この認証サーバ1は、サーバ本体と、コンピュータ読み取り可能な記録媒体に記録されているコン

ピュータプログラムとによって実現される。コンピュータプログラムは、通常は、サーバ本体が具える記録装置に記録され、サーバ本体のＣＰＵがその記録装置から適宜読み出して実行するようになっているが、ＣＤ－ＲＯＭやＤＶＤ－ＲＯＭのような可搬性の記録メディアに記録されているものであっても良い。あるいはコンピュータネットワークを通じてダウンロードされるものであっても良い。図7は、サーバ本体のＣＰＵが、上記のコンピュータプログラムを読み込んで実行することによって形成される機能ブロック図である。本実施形態では、出入力部３１と処理部３２とを形成するようにする。出入力部３１は、ユーザ端末Ｔ１との間、或いはホストサーバ１０との間のデータの出入を制御しながら通信を行う。より具体的には、例えば、ユーザ端末Ｔ１を操作するユーザからの認証用情報を受け付け、認証の結果をユーザ端末Ｔ１に返信して、その後のデータの出入を制御したり、認証の結果をホストサーバ１０に通知したりする。後者の場合は、ユーザ端末Ｔ１の以後のアクセスをホストサーバ１０に導くことも行う。

【００３８】処理部３２は、認証及び認証に関わる処理を行うもので、出入力部３１との間でデータを受け渡しできるようになっている。この実施形態では、図7に示すように、制御部３２ａ、プログラム送信部３２ｂ、認証部３２ｃ、識別情報記録部３２ｄ、送出情報管理部３２ｅ、及び送出情報記録部３２ｆの機能を備えて処理部３２を構成している。

【００３９】制御部３２ａは、装置全体の基本的な動作の制御を行う。プログラム送信部３２ｂ、認証部３２ｃ、情報記録部３２ｄ、送出情報管理部３２ｅ、及び送出情報記録部３２ｆは、いずれも、この制御部３２ａの管理下で動作を行う。制御部３２ａは、また、本発明における許可手段の機能の一部をも併有しており、後述する認証部３２ｃが、認証を求めるユーザ端末Ｔ１を正当なものと認証した場合、ユーザ端末Ｔ１によるサーバ１０の共通ファイルの記録情報へのアクセスを許可するようになっている。制御部３２ａは、また、送出情報記録部３２ｄに記録された後述のデータに基づいて、各ユーザ端末Ｔ１についての送出情報を、当該ユーザ端末のディスプレイに表示するためのデータを生成する機能をも有している。この点で、制御部３２ａは、送出情報提示手段としての機能も有している。

【００４０】プログラム送信部３２ｂは、アクセスの要求がユーザ端末Ｔ１からあった場合に、当該ユーザ端末に、例えばＪａｖａで記述されたプログラムを送信するものである。このような送信は、上述の出入力部３１を介して行われる。このプログラムは、認証の対象となるユーザ端末Ｔ１から上記の識別情報を送信させるためのプログラムである。

【００４１】認証部３２ｃは、ユーザ端末Ｔ１からのアクセス要求が認証サーバ１に届いた場合に、そのユーザ端末Ｔ１が適正なものか否かについての判断を行う。認証部３２ｃは、具体的には、出入力部３１を介して受け付けた、認証を求めている当該ユーザ端末Ｔ１から入力された認証用情報と情報記録部３２ｄに記録されている認証用情報との整合性を見ることでその判断を行う。そのために、情報記録部３２ｄには、認証の対象となる複数のユーザ端末Ｔ１のすべてについての認証用情報が記録されている。

【００４２】認証用情報の一例を図8に示す。ここでは、単純な例として、ユーザＩＤ（ＵｓｅｒＩＤ）とパスワード（PASSWORD）の組、及び各ユーザ端末Ｔ１のそれぞれが通信を許可される範囲情報の一例となる認証ＵＲＬ（例えば所望のホストサーバ１０のＵＲＬ）が、それぞれユーザ端末Ｔ１の識別情報の一例である個体番号と、原則として１対１の対応関係で認証テーブルとして記録されている。但し、一つの個体番号に対して２以上のユーザＩＤが割振られている場合には、そのユーザＩＤのそれぞれについて、異なる認証ＵＲＬが割振られている。図8の例でいえば、個体番号００１０２に対して２つのユーザＩＤが割振られており、そのそれぞれに対して異なる認証ＵＲＬが割振られている。ユーザＩＤ及びパスワードは、数字のみ、アルファベットのみ、あるいはこれらの組み合わせからなり、システムの管理者が事前に割り当てるか、各ユーザが予め決定したものである。

【００４３】図8に示した認証テーブルの例では、認証ＵＲＬと、ユーザＩＤ及びパスワードの組とが、原則として１対１に対応しているから、ユーザは、アクセスする認証ＵＲＬに応じて、現在知っているユーザＩＤ／パスワードでログインすれば良い。従って、ログイン時の処理が単純化されるため、一つのユーザ端末Ｔ１（個体番号）で一つ又は二つ程度のホストサーバ１０（認証ＵＲＬ）との対応関係のみを考慮すれば良い簡易なシステムでは、好ましい認証形態となり得る。

【００４４】しかし、ユーザが、一つのユーザ端末Ｔ１で複数のホストサーバ１０にアクセスしてサービス提供を受けたり、一つのホストサーバ１０内に複数のサービス用プログラムがあってそのそれぞれについて認証が必要となる場合は、ホストサーバ毎、あるいはサービス用プログラム毎にログイン画面を作成したり、ユーザＩＤ及びパスワードを保持したりしなければならないため、システムの維持管理が煩雑となる。また、ユーザがユーザ端末Ｔ１をなくしてしまったり、盗難にあったりして、そのユーザＩＤ及びパスワードを使えなくなるようにする場合には、それを、認証テーブルに記録されているすべてのホストサーバ、あるいはサービス用プログラムについて行わなければならないため、煩雑となる。

【００４５】従って、一つのユーザ端末Ｔ１で多数のサービス提供を受ける可能性がある大規模システムの場合は、例えば図９（ａ）に示す認証マスタテーブルと、図

９（ｂ）に示す認証テーブル（図8のものと同じ）とを用いて認証用のデータを階層的に管理する形態が望ましい。認証マスタテーブルは、個体番号でリンクする認証テーブルの上位テーブルとなるもので、一つの個体番号に対して一つのフィールドが用意されている。個々のフィールドには、認証ＩＤ、認証パスワード（認証ＰＳＷ）、当該ユーザ端末用の停止フラグの記録領域（停止）が形成される。

【００４６】認証ＩＤは、そのユーザ端末Ｔ１について一つだけ割り当てられるマスタＩＤとなるＩＤ情報であり、図９（ｂ）（図８）の認証テーブルに複数のユーザＩＤが記録されている場合であっても、それを用いることで認証を正当とするために使用される。認証パスワードも同様である。停止フラグの記録領域は更新自在の領域であり、フラグ「１」がたっている場合は、そのユーザ端末Ｔ１についての認証テーブルの使用をすべて停止させるために使用される。停止解除時には、フラグ「１」を消去することで、認証テーブルを使用できるようになる。

【００４７】このように、二つのテーブルを階層的に使用することで、ユーザは、アクセスできるホストサーバ１０やサービス用プログラムが複数であっても、認証ＩＤと認証パスワードのみを知っていれば良くなり、アクセス時の作業が簡略化される。また、ホストサーバ毎、あるいはサービス用プログラム毎にログイン画面を作成する必要がなく、さらに、ユーザ端末Ｔ１をなくした場合であっても、停止フラグの記録領域に「１」をたてるだけで足りるので、システムの維持管理作業も簡略化される。

【００４８】認証部３２ｃは、ユーザ端末Ｔ１から受け付けた識別情報（例えば自動的に送られる個体番号）と情報記録部３２ｄに記録されている識別情報（個体番号）とを比較し、また、ユーザ端末Ｔ１から受け付けたユーザＩＤ又は認証ＩＤと情報記録部３２ｄに記録されているユーザＩＤ又は認証ＩＤとを比較し、さらに、ユーザ端末Ｔ１から受け付けたパスワードと情報記録部３２ｄに記録されたパスワード又は認証パスワードとを比較する。そして、受け付けた識別情報、ユーザＩＤ（認証ＩＤ）、パスワード（認証パスワード）の組が、あるユーザ端末Ｔ１についての識別情報、ユーザＩＤ（認証ＩＤ）、パスワード（認証パスワード）と一致している場合には、アクセスを求めてきたユーザ端末Ｔ１が正当なものと認証する。正当である旨を表す情報は、上記の認証テーブルで対応付けられた認証ＵＲＬの情報と共に制御部３２ａへ送られる。これを受け付けた制御部３２ａは、そのユーザ端末Ｔ１からのアクセスを該当する認証ＵＲＬに導く。これにより、アクセスしてきたユーザ端末Ｔ１と目的のホストサーバ１０との間の通信が可能になる。

【００４９】送出情報管理部３２ｅは、送出情報記録部３２ｆに記録するデータを管理する。送出情報管理部３２ｅは、ホストサーバ１０からユーザ端末Ｔ１へと送出された情報を抽出し、いかなる情報が送出されたかという送出情報を生成した上で、これを各ユーザ端末Ｔ１と対応付けて、送出情報記録部３２ｆへ記録するようになっている。この点で、送出情報記録部３２ｆは、抽出部としての機能を有している。また、送出情報管理部３２ｅは、送出情報記録部３２ｆに記録されたデータを、読み出す機能をも持ち合わせている。読み出されたこのデータは、制御部３２ａへと送られ、送出情報を視認可能な状態でユーザ端末Ｔ１のディスプレイに表示するためのデータを生成するために用いられる。このデータは、出入力部３１を介してユーザ端末Ｔ１へと送られるようになっている。

【００５０】＜運用形態：情報アクセス方法＞上記のように構成されるネットワークシステムの運用形態は、例えば、以下のようになる。上述のようにイントラネットＬＮのセグメントＳａ～Ｓｅは、それぞれ管理対象となるユーザ企業のホストサーバ用に割り当てられているので、セグメント単位でユーザ企業の利用に供することができる。ユーザ企業に供する利用の形態は、セグメントＳａ～Ｓｅのみであっても良く（この場合は、ユーザ企業が、ホストサーバ１０とこのホストサーバ１０に対応するローカルサーバ２０を持ち込む）、所定の機能を搭載したホストサーバ１０が配備されたセグメントＳａ～Ｓｅであっても良い。後者は、ユーザ企業が、ホストサーバ１０に対応するローカルサーバ２０を既に保有している場合に適する。

【００５１】管理対象となるユーザ企業、セグメント及びイントラネットＬＮ内に配備するホストサーバ１０が決まると、システム管理者は、ファイアウォール１１に、発信端末からのアクセスを通過させるための各種条件（プロトコル、システム固有のデータフォーマット、ホストサーバ１０のアドレス等）を登録し、さらに、イントラネットＬＮ内のルータ１３のアドレステーブルに、イントラネットＬＮ内の宛先及び発信元としてホストサーバ１０のアドレスを登録しておく。また、スイッチングハブ１４の接続元にホストサーバ１０のアドレスを登録する。更に、認証サーバ１中の情報記録部３２ｄに、各ユーザ端末Ｔ１毎の、識別情報、ユーザＩＤ（又は認証ＩＤ）、パスワード（又は認証パスワード）、認証ＵＲＬについての各データを記録する。

【００５２】ユーザ企業の構成員（通常は、社員）は、ユーザ端末Ｔ１を操作して、ＩＰアドレス（例えば、×××@×××.co.jp）で所望のホストサーバ１０に情報アクセスを行うことになる。このアクセスは、無線網ＷＮから携帯電話網ＭＮに接続されたＤＮＳ３０に転送される。ＤＮＳ３０は、当該アクセスに含まれるドメイン名をもとにグローバルＤＮＳ４０から当該ユーザ企業用のグローバルなＩＰアドレス（例えば、2××.111.2

2.33）を取得し、これをルータ１２に転送する。

【００５３】ルータ１２は、図４（ａ）の内容のＮＡＴテーブルを参照して、ＤＮＳから与えられたグローバルなＩＰアドレスをホストサーバ１０のＩＰアドレス（1××.111.22.33）に変換し、同時にユーザ端末Ｔ１のグローバルＩＰアドレス（2××.444.55.6）をＩＰアドレス（1××.444.55.6）に変換する。そして、ルーティング機能を用いて、当該アクセスをファイアウォール１１へと転送する。ファイアウォール１１は、このアクセスが予め登録されている条件に適合しているかどうかを判定し、適合している場合には、それを通過させ、認証サーバ１に転送する。認証サーバ１は、アクセス要求をしてきた当該ユーザ端末Ｔ１が適正なものか否かを判定し、それが適正なものであると認証した場合には、当該アクセスをルータ１３に送る。

【００５４】ルータ１３は、このアクセスの内容を解読して該当するセグメント及びホストサーバ１０を割り出し、そのホストサーバ１０にアクセスを転送する。ホストサーバ１０は、アクセスの要求に応じたデータを共通ファイルから検索し、これをルータ１３、認証サーバ１及びファイアウォール１１を介してルータ１２に返信する。ルータ１２は、図４（ｂ）の内容のＮＡＴテーブルを参照して、ホストサーバ１０のアドレスをユーザ端末Ｔ１のＩＰアドレスに変換し、ルーティング機能を用いて返信データを公衆通信網ＤＮ及び無線網ＷＮを介してユーザ端末Ｔ１に転送する。

【００５５】ホストサーバ１０とローカルサーバ２０との間では、専用回線網ＰＮを介して複写タスクが実行されており、両者の共通ファイルの内容の同一性が維持されているので、上記のホストサーバ１０から返信される情報は、ローカルサーバ２０の保有情報と同じ内容となる。従って、このネットワークシステムを利用することで、セキュリティ性が確保された低コストの企業専用システムを容易に実現することができる。特に、その位置が特定されないユーザ端末Ｔ１からローカルサーバ２０の保有情報（メールファイル、スケジュールファイル等）をセキュアに知得できるので、あたかも、ユーザ端末Ｔ１とローカルサーバ２０とが専用回線で結ばれたようになり、第三者の介入がないので、社内情報を扱う上では極めて都合が良い。また、このネットワークシステムによれば、例えば企業の本社のローカルサーバと複数の支店の各々のローカルサーバが扱う情報をすべて共通ファイル化し、これをイントラネットＬＮ内のホストサーバで一元的に管理しておいて、この共通ファイルにユーザ端末Ｔ１から任意の時点で任意の箇所からアクセスできるようにすることにより、矛盾のない社内情報に統一的な操作でアクセスできるようになり、企業におけるグループウェアの好ましい運用形態が容易に実現される。

【００５６】＜応用例１：社内メーリングシステム＞次に、ネットワークシステムの応用例を説明する。ここでは、イントラネットＬＮの特定のセグメントを、あるユーザ企業に割り当て、ユーザ端末Ｔ１を用いて当該ユーザ企業の社内情報にアクセスする社内メーリングシステムに応用した場合の例を挙げる。ここにいう「メール」は通常の電子メール文書のみならず、種々のリストデータや編集されたデータ及び予め登録されている種々の文書をも含む概念である。また、使用可能な文字数や蓄積件数に制限がない、文書添付が可能なウエブメールである。ウエブメールを用いることにより、ユーザ端末Ｔ１の機種に依存しない統一的な操作でメールの受け渡しを行うことができる。

【００５７】ユーザ端末Ｔ１は、例えば株式会社エヌ・ティ・ティ・ドコモ（ＮＴＴドコモ）が提供する「ｉ－ｍｏｄｅ端末」のように、それ自体でウエブメール機能を有するユーザ端末となり得る携帯電話が普及しているので、これを用いることができる。但し、メールサーバは「ｉ－ｍｏｄｅ（登録商標）端末」用のｉ－ｍｏｄｅサーバではなく、ホストサーバ１０が用意するウエブメールサーバ機能を用いる。これにより、「ｉ－ｍｏｄｅ端末」が標準的に具備するブラウザ機能の操作環境をそのまま利用しつつ、ｉ－ｍｏｄｅサーバによる各種使用の制限、例えば送受信できるデータの種類やサイズ、件数等の制限を解除することができるようになる。また、機種の相違を吸収した統一的な操作環境を実現することができるようになる。

【００５８】ホストサーバ１０及びローカルサーバ２０としては、米国ロータス社が提供する「ＤＯＭＩＮＯサーバ（ＤＯＭＩＮＯ（又はDomino）は同社商標、以下同じ）」を搭載したコンピュータを用いることができる。「ＤＯＭＩＮＯサーバ」には、本発明を実施する上で好適な機能、例えば通信機能、メール機能、サーバ機能（特にＨＴＴＰサーバ機能）、スケジュール機能、複写機能が標準搭載されており、また、既存の機能を改良するためのプログラミングが許されているので、これを利用することが便利である。本発明の実施に適したウエブメールサーバ機能、例えば社内メール専用のメニューリストを編集したり、文書毎に料金情報を付加したり、大容量のデータを受信先のメモリ容量に応じて自動的に分割して送付したり、添付文書を携帯電話の限られた表示領域に縮小して表示したり、メールの宛先が多い場合にその表示を規制して本文のみを表示させたりすることは、「ＤＯＭＩＮＯサーバ」が具備する標準的なメール機能に別途アプリケーションプログラムを追加作成することで、容易に実現することができる。また、スケジュール機能として、現在時刻を常に監視しておき、現在時刻後のスケジュールについてのみ抽出する機能も、別途アプリケーションプログラムを追加作成することで、それを容易に実現することができる。

【００５９】「ＤＯＭＩＮＯサーバ」を用いたホストサ

ーバ10の機能構成図を図5に示す。このホストサーバ10は、所定のOS（オペレーティングシステム）の管理下で動作するCPU101と、RAM102と、ROM103と、CPU101が読み取り可能なハードディスク等の固定記憶装置に構築されるメールファイル104、メールアドレス帳や社員の個人情報を記録した社員データベース105、HTTP文書等を記録した文書データベース106、社内スケジュールデータを記録したスケジュールファイル107と、ルータ13等との間の通信制御を行う通信アダプタ108とを具備している。RAM102には、DOMINOサーバが標準装備するDOMINOエンジン、複製タスク、HTTPタスク、スケジュール管理タスクのほか、社員用のウエブメールサーバ機能を実現するためのプログラムが格納される。ROM103には、BIOS（Basic Input Output System）を含む制御プログラム等が記録されている。DOMINOエンジンは、プラットホームやネットワークOSの違いを吸収して統一的な操作環境を提供するもので、文書の統合、検索を含む強力な文書管理機能を実現することができる。

【0060】HTTPタスクは、携帯電話からHTTP送信要求を受け付けたときに、当該HTTP送信要求に対応するデータファイルを特定し、これをHTML形式に変換するタスクである。拡張URLを利用できるため、HTTP送信要求に対応するデータファイルをダイナミックにHTML形式に変換することができる。ローカルサーバ20も、上記のDOMINOサーバを用いることができる。

【0061】ホストサーバ10とローカルサーバ20は、図6に示す複製タスクによって、互いに共通ファイルの同一性を維持するようになっている。すなわち、それぞれのディレクトリのコンフィグレーションに基づき、一定時間間隔で複製タスクを起動し、自己の共通ファイルが相手側の共通ファイルと差異がないかどうかと比較する。差異があれば双方向に差分データを転送し合い、それを自己の共通ファイルの内容に反映させる。複製は、図示のようにフィールド単位で行われる。変更されたフィールドのみを複写する点で、通常の「ファイルコピー」とは異なる。

【0062】次に、図10～図29を参照して、社内メールシステムの使用形態を説明する。

（事前準備）予め、ローカルサーバ20個のクライアント端末（図示省略）を操作して、ユーザIDとパスワードの組を許可情報として設定しておく。なお、この例ではユーザIDとして社員IDを用いるものとする。設定された内容は、ホストサーバ10の社員データベース105に反映される。ここで設定されるのは、携帯電話からイントラネットLN内にアクセスするときの認証と、課金の際に必要となる情報である。この例の社員ID又はパスワードには、グループ（部門）毎の課金を可能にするために、グループ毎の識別データが割り当てられている。携帯電話を利用した場合の課金は、データ総量（パケットサイズの総量）に応じてなされるので、これを識別データ毎に集計できるようにしておく。社員データベース105には、また、携帯電話のアドレスを予め設定しておく。また、識別情報、ユーザID、パスワード、認証URLの情報を認証サーバ1に設定しておく。

【0063】（携帯電話用のアドレス帳作成）社員データベース105の社内アドレス帳から10名分程度のアドレスを抜き出し、これを随時、携帯電話に送出できるようにしておく。これは、原則として上記のクライアント端末で行う。この場合の手順を図10及び図11に示す。図10を参照し、まず、クライアント端末の表示装置に社内アドレス帳のユーザアドレス一覧を表示させる（S101）。クリックイベント（表示されているイベントのうち操作者のクリック操作により選択されたもの、以下同じ）の発生を待ち（S102）、クリックイベントは発生した場合はその内容を判定する（S103）。クリックイベントが「選択欄」の場合は、ユーザアドレス一覧の中から、特定の者の前に選択マークを表示してS103の処理に戻る（S104）。「コピーボタン」の場合は、選択マークがついた者のデータを個人アドレス帳にコピーしてS101の処理に戻る（S105）。「終了ボタン」の場合は終了処理を行う（S106）。これにより、数人分のアドレスからなる個人アドレス帳が生成される。

【0064】個人アドレス帳から実際に使用するアドレスを抜き出す場合は、図11の手順で処理を行う。まず、クライアント端末のディスプレイに、上記の個人アドレス帳のユーザアドレス一覧を表示させる（S201）。クリックイベントの発生を待ち（S202）、クリックイベントが発生した場合はその内容を判定する（S203）。クリックイベントが「選択欄」の場合は、ユーザアドレス一覧の中から特定の者の前に選択マークを表示してS203の処理に戻る（S204）。「コピーボタン」の場合は選択マークがついたデータを順にメールファイルにコピーしてS201の処理に戻る（S205）。「終了ボタン」の場合は終了処理を行う（S206）なお、社内アドレス帳からのアドレスを抜き出して携帯電話用のアドレス帳を作成する処理は、携帯電話からも行うことができる。但し、この場合は、個人アドレス帳に一度コピーするのではなく、直接、社内アドレス帳から選択することになる。

【0065】（認証及び情報アクセス）次に、ユーザ企業の構成員が携帯電話からホストサーバ10にアクセスする場合の操作手順を説明する。図12は、情報アクセス方法の全体的な手順説明図である。まず、携帯電話がアクセス要求を行う。アクセス要求と同時に、携帯電話から認証サーバに接続要求先についてのURLが送られる。次いで、携帯電話の表示部にログイン画面が表示さ

れる（S301）。ログイン画面には図26（a）に示されるように、ユーザID（ここでは社員ID）とパスワードの入力領域51が表示される。ユーザIDとパスワードが入力された場合は、ログインの認証を行う（S302）。認証失敗の場合はS302に戻る。認証が成功した場合、つまり正規ユーザであった場合はメイン画面を表示する（S303：Yes、S304）。メイン画面は、例えば図26（b）に示されるものであり、受信/送信/検索/予定のイベント選択領域52とSUBMIT選択領域53が表示される。

【0066】上述したログインの認証について、図13を用いて詳しく説明する。図13は、ログインの認証時に認証サーバ1で行われる処理の手順を示したものである。ログイン画面が表示されると（S301）、認証サーバ1は、その携帯電話が有する識別情報を読み出してこれを認証サーバ1へと送信させるための上述のプログラムを、その携帯電話へと送信する（S3011）。より詳しく説明すると、アクセス要求があった旨の情報は、出入力部31を介して制御部31aへと送られる。これを受け付けた制御部31aは、プログラムの送信を行うようにとの命令を、プログラム送信部32bへと送る。この命令に基づいて、プログラム送信部32bは、出入力部31を介して携帯電話へ上述のプログラムを送信する。この例において上述のプログラムは、例えばJavaで記述されたものであり、携帯電話のKVM上で実行される。いずれにしても、携帯電話に準備された実行環境下で動作するものである。このプログラムは、携帯電話が持っている識別情報をROMなどから読み出すプログラムを起動させる。これにより生成された機能実現体が、ROMなどから読み出した識別情報を認証サーバ1へ送る。この過程は自動的に行われる。このようにして識別情報を受け付けると（S3012）、認証サーバ1は、この識別情報が、情報記録部30dに記録されている識別情報のいずれかと一致するか否かを認証部32cで判定する（S3013）。受け付けた識別情報が、記録されていた識別情報のいずれとも一致しない場合（S3013：No）には、その旨を示す情報を携帯電話のディスプレイに表示させるためのデータを生成し、これを携帯電話に送る（S3014）。この場合には、当該携帯電話が正規なものであるとの認証はなされず、携帯電話からの当該アクセスは認められないことになる。なお、この実施形態では、携帯電話のディスプレイに画像を表示させるためのデータの生成は、制御部32が行う。受け付けた識別情報が記録されていた識別情報のいずれかと一致する場合（S3013：Yes）には、次のステップに進む。

【0067】次いで、ユーザが入力したユーザID及びパスワードを携帯電話から受け付け（S3015）、このユーザID及びパスワードが、情報記録部30dに記録されているユーザID及びパスワードのうち、上述の識別情報と対応付けられたものと一致するか否かを、認証部32cで判定する（S3016）。なお、ユーザID及びパスワードの携帯電話からの受付（S3015）は、識別情報の受付とは独立に行われるため、ステップS3011よりも先に実行される場合がある。受け付けたユーザID及びパスワードが、情報記録部30dに記録されているユーザID及びパスワードのうち、上述の識別情報と対応付けられたものと一致しない場合（S3016：No）は、その旨を示す情報を携帯電話のディスプレイに表示させるためのデータを生成し、上述の場合と同様にこれを携帯電話に送る（S3014）。受け付けたユーザID及びパスワードが、情報記録部30dに記録されているユーザID及びパスワードのうち、上述の識別情報と対応付けられたものと一致する場合（S3016：Yes）には、次のステップに進む。

【0068】識別情報、ユーザID及びパスワードが互いに対応付けられて情報記録部30dに記録されていた識別情報、ユーザID及びパスワードと一致した場合には、アクセス要求をしてきた携帯電話が正規なものであるとの認証をしても良いが、この実施形態では、認証の確実性を更に増すべく、以下のような処理を行うこととしている。すなわち、先に受け付けていた接続要求先のURLが、情報記録部30dに記録されている認証URLのうち、受け付けた識別情報及びユーザIDと対応付けられたものと一致するか否かの判定を行う（S3017）。この判定も、認証部32dが行う。受け付けたURLが、情報記録部30dに記録されている認証URLのうちの、受け付けた識別情報及びユーザIDと対応付けられたものと一致しない場合（S3017：No）には、上述の場合と同様に、S3014へ進むことになる。一致する場合（S3017：No）には、その携帯電話を正規なものとして認証しポートを開放する（S3018）。

【0069】次いで、クリックイベントの発生を待ち（S302）、クリックイベントが発生した場合はその内容を判定する（S303）。クリックイベントが「受信」であった場合は、図14～図19の手順で受信処理を行う（S304）。「送信」であった場合は図20の手順で送信処理を行う（S305）。「検索」であった場合は図21～図23の手順で検索処理を行う（S306）。「予定」であった場合は、図24及び図25の手順で予定処理を行う（S307）。これらの処理が終了した場合は、ステップS302の処理に戻る。以下、受信処理、送信処理、検索処理、予定処理の内容を、詳細に説明する。

【0070】＝受信処理＝

S304の受信処理について説明する。受信処理では、図14に示されるように、携帯電話の受信ボックスの受信日で降順にソートし、1から順に「＋1」でデータ番号を採番する（S401）。ソートされたデータを昇順

に10件ずつ選択し、1件目をSTART（最初のデータ番号、以下同じ）に設定する（S402）。その後、選択されたデータを受信一覧表示領域に表示させる（S403）。受信一覧表示領域には、図26（c），（d）に示されるように、件名領域54とその件の受信に要する料金情報を表す料金領域55とが対となって表示される。このように受信に要する料金情報を表示させることで、携帯電話の操作者にデータのサイズと、そのときのコストとを知らしめることができる。携帯電話の操作者（つまり社員）は、件名タイトルと料金額を見てその件を読むことがコストに見合った内容かどうかを判断したり、料金額から受信に要する時間を推測してその件を今読むべきものか後で読んだ方が良いかどうかを判断したりすることが可能になる。また、例えば2万ワードもあるような大量のデータは、ウエブメール機能によって自動的にメール分割されながら送られるので、途中までそれを閲覧して、以後の分割メールの閲覧を中止するような利用形態も可能になる。受信一覧表示領域の下部には、「前へ」及び「次へ」の選択ボタンも表示される。クリックイベントの発生を待ち（S404）、クリックイベントが発生した場合はその内容を判定する（S405）。クリックイベントが「次へ」であった場合は、「+9」をSTARTに設定し（S406）、STARTから10件を選択する。STARTが10未満のときは存在するデータのみを表示させる（S407）。クリックイベントが「前へ」であった場合は、「-9」をSTARTに設定し（S408）、STARTから10件を選択する。STARTが10未満のときはSTARTに「1」を設定する（S409）。クリックイベントが「文書番号」であった場合は、受信文表示処理を行う（S410）。

【0071】S410の受信文処理の詳細は、図15に示すとおりである。携帯電話の操作者が表示部の所望の文書番号をクリックしたことを検知すると（S501）、クリックされた文書番号の文書を表示部に表示させる（S502）。このときの表示は、例えば図26（e）のようになる。なお、添付文書がある場合は、その存在を示す通知を表示部に表示させる。これは、ホストサーバ10のウエブメールサーバ機能による。添付文書が表オブジェクトやビットマップデータの場合は、添付文書の表記をクリックすることで、それをHTML文書として表示領域のサイズに併せて表示させることができる。また、文書の宛先数が多い場合を想定して、予め受信文のフレームの中の宛先部分を表示させないようにする。これにより、携帯電話の表示部には、本文のみを表示させることができる。但し、宛先の情報についてはホストサーバ10の側で管理されているので、携帯電話から宛先を確認したい場合には、それをブラウザ画面（アイコン又はコマンド文字を用意しておく）から指示することによって、表示させることはできる。受信文処理の場合、表示部の上部には、「削除」、「返信」、「転送」、「FAX」の選択領域56が表示される。クリックイベントの発生を待ち（S503）、クリックイベントが発生した場合は、その内容を判定する（S504）。クリックイベントには、「削除」処理（S505）、「返信」処理（S506）、「転送」処理（S507）、「FAX」処理（S508）がある。

【0072】ステップS505の「削除」処理、すなわち図26（e）の表示内容で「削除」が選択された場合の処理の手順は、図16のようになる。現在の文書を削除するとともに（S601）、削除済みを表す「Deleted」を表示させる（S602）。

【0073】ステップS506の「返信」処理、すなわち図26（e）の表示内容で「返信」が選択された場合の処理の手順は、図17のようになる。まず、返信用の新規文書を作成する（S701）。そして、その宛先に受信文書の送信者を設定するとともに（S702）、件名に受信文書の件名の先頭に「Re：」の文字を付加し（S703）、その新規文書を表示させる（S704）。クリックイベントの発生を待ち（S705）、クリックイベントが発生した場合はその内容を判定する（S706）。クリックイベントが「件名」の場合は件名編集処理を行い（S707）、「内容」の場合は文書内容の編集処理を行い（S708）、「新規宛先」の場合は新規宛先編集を行い（S709）、「CC新規」の場合はCC（カーボンコピー）先の新規編集処理を行う（S710）。それぞれ、終了後はS705の処理に戻る。

【0074】ステップS706で判定したクリックイベントが「宛先」の場合は、宛先編集処理を行うが（S711）。このとき、モバイル個人宛先（個人アドレス帳）の一覧を表示する（S712）。そして、選択された宛先を「TO」として設定する（S713）。その後、S705の処理に戻る。クリックイベントが「CC」の場合はCC宛先編集処理を行う（S714）。このとき、モバイル個人宛先（個人アドレス帳）の一覧を表示する（S715）。そして、選択された宛先を「CC」として設定する（S716）。その後、S705の処理に戻る。クリックイベントが「SUBMIT」の場合は当該新規文書を送信し（S717）、「Formprocessed」を表示して返信処理を終える（S718）。

【0075】ステップS507の「転送」処理、すなわち図26（e）の表示内容で「転送」が選択された場合の処理の手順は、図18のようになる。処理内容（S801～S818）は、概ね図17の場合と同様であり、S803で、件名に受信文書の件名の先頭に「FW：」の文字を付加する点のみが異なる。

【0076】ステップS508の「FAX」処理、すなわち図26（e）の表示内容で「FAX」が選択された場合の処理の手順は、図19のようになる。まず、FA

X用の新規文書を作成する（S901）。そして、その内容欄に受信文書の内容を設定するとともに（S902）、件名に受信文書の件名の先頭に「FW：」の文字を付加し（S903）、その新規文書を表示させる（S904）。クリックイベントの発生を待ち（S905）、クリックイベントが発生した場合はその内容を判定する（S906）。クリックイベントが「件名」の場合は件名編集処理を行い（S907）、「FAX番号」の場合はFAX番号編集処理を行い（S908）、それぞれ、終了後はS905の処理に戻る。クリックイベントが「送信」の場合は当該新規文書を送信し（S909）、「Formprocessed」を表示してFAXデータ送信処理を終える（S910）。このようにして送信されたデータは、FAX番号先でFAX印刷される。なお、上記のFAX印刷は、DOMINOエンジンの機能の一つとして実現しても良く、別途、FAX印刷用のアプリケーションプログラムをホストサーバ10に搭載しておき、これを随時起動することによって実現しても良い。

【0077】＝送信処理＝

次に、ステップS305の送信処理について説明する。送信処理では、図20に示すように、送信用の新規文書を作成し（S1001）、その新規文書を表示部に表示させる（S1002）。その後の処理（S1003～S1016）は、図17に示した返信処理のステップS707～S718と同様の手順となる。但し、携帯電話の表示部の表示内容は、図26（f）のように変わる。

【0078】＝検索処理＝

次に、ステップS306の検索処理について説明する。検索処理は、図27（a）のように、ユーザが「検索」を選択した場合に実行される。この処理は、図21に示されるように、まず、検索ビュー内のデータをアルファベットで昇順にソートし、10件を選択する（S1101）。その後、検索リストを一覧表示領域に表示させる（S1102）。クリックイベントの発生を待ち（S1103）、クリックイベントが発生した場合はその内容を判定する（S1104）。クリックイベントが「次へ」であった場合は、表示中の頁の10件目から＋10のデータを設定する（S1105）。その後、設定した分のデータを選択するが、データが10未満のときは存在するデータのみを選択する（S1106）。その後、S1102の処理に戻る。クリックイベントが「前へ」であった場合は、表示中の頁の10件目から－10のデータを設定する（S1107）。その後、設定した分のデータを選択するが、データが存在しないときは現頁のデータを再選択する（S1108）。その後、S1102の処理に戻る。

【0079】クリックイベントが「検索リスト表示」であった場合、携帯電話の表示部の表示内容は、図27（a）から過去に検索したキーワード一覧に変わる。図27（b）は、この様子を示している。図27中、「itoh」、「okada」、「suzuki」は、検索したキーワードである。この検索リスト表示処理の手順は、図22に示されるとおりである。すなわち、クリックイベントの発生を待ち（S1201）、アルファベットの姓名（例えば「itoh」）がクリックされたことを検知した場合は当該クリックされた姓名を含むすべての文書を表示させる（S1202，S1203）。

【0080】クリックイベントが「新規キーワード」であった場合は、新規キーワードによる検索処理を行う。このとき、表示部の表示内容は、図27（c）のように、新規キーワードの入力画面に変わる。この場合の処理は、図23に示されるように、クリックイベントの発生を待ち（S1301）、クリックイベントが発生した場合はその内容を判定する（S1302）。クリックイベントが「新規キーワード」の場合は、新規キーワード編集を行い（S1301）、S1301の処理に戻る。クリックイベントが「SUBMIT」の場合は当該キーワードを送信し（S1304）、「Formprocessed」を表示して処理を終える（S1305）。ホストサーバ10から検索結果が送信された場合は、適宜、検索リスト表示処理に移る。表示部の画面は、図27（d）のように変わり、アルファベット（例えば「pat」）がクリックされた場合は、図27（e）のように「pat」を含むすべての文書が表示される。

【0081】＝予定処理＝

次に、ステップS307の予定処理について説明する。予定処理は、図28（a）のように、ユーザが「予定」を選択した場合に実行される。この処理は、図24に示されるように、まず、予定ビュー内のデータを日付で降順にソートして、10件を選択し（S1401）。その後、予定リストを表示部の一覧表示領域に表示させる（S1402）。図28（b）は一覧表示領域60の例であり、ある日付がクリックされることによって、その日付に設定されている時間帯と簡単な説明とが表示される様子が示されている。表示部の上部には、「前へ」、「次へ」、「作成」のイベントを選択するための領域が形成される。クリックイベントの発生を待ち（S1403）、クリックイベントが発生した場合はその内容を判定する（S1404）。クリックイベントが「次へ」であった場合は、表示中の頁の10件目から＋10のデータを設定する（S1405）。その後、設定した分のデータを選択するが、データが10未満のときは存在するデータのみを選択する（S1406）。その後、S1402の処理に戻る。クリックイベントが「前へ」であった場合は、表示中の頁の10件目から－10のデータを設定する（S1407）。その後、設定した分のデータを選択するが、データが存在しないときは現頁のデータを再選択する（S1408）。その後、S1402の処理に戻る。なお、予定ビュー内のデータは、「今日の日付」以降のもののみが対象となる。つまり、スケジュー

ルファイル107から当該日付以降に予定があるものを抜き出し、これをリスト（DOMINOサーバにおけるView）にして携帯電話で見れるようにする。このようにすれば、携帯電話に過去の予定に関するデータが記録される事態を防止することができ、携帯電話が有するメモリの有効活用が可能になる。当該日付以前及び現在時刻以前の予定に関するデータをホストサーバ10のスケジュールファイル107から自動的に削除するように構成しても良い。この場合には、不要なデータがスケジュールファイル107（ローカルサーバ20のものも同様）から逐次削除されるので、ホストサーバ10（ローカルサーバ20も同様）のメモリ領域の有効活用も同時に図れるとともに、社内情報の漏洩が確実に防止される利点がある。

【0082】クリックイベントが「新規作成」であった場合、すなわち図28（c）の表示内容で「作成」が選択された場合は、予定リストの新規作成処理に移行する。図25は、新規作成処理の手順図である。この処理では、まず、予定作成メニューを表示する（S1501）。予定作成メニューには、例えば図28（d）に示されるように、予定登録、会議召集、イベント、確認、記念日の選択領域61が形成される。ユーザがこれらのいずれかを任意に選択できるようになっている。クリックイベントの発生を待ち（S1502）、クリックイベントが発生した場合はその内容を判定する（S1503）。選択領域61から特定のメニューが選択された場合は、データ入力、編集を行い（S1504）、S1502の処理に戻る。クリックイベントが「SUBMIT」の場合は当該入力したデータを送信し（S1505）、「Formprocessed」を表示して処理を終える（S1506）。図28（e）は、「2．会議召集」が選択された場合のデータ入力領域62の内容例を示した図である。日付毎に、簡単な説明と時間が対応付けられている。なお、データ入力領域62は、スクロールするようになっている。このようにして入力されたデータは、ホストサーバ10のスケジュールファイル107に反映され、さらに、ローカルサーバ20にも反映される。

【0083】なお、予定処理の一環として、あるいは予定処理とは別の処理として、いわゆる「To Do リスト」機能、つまり遂行すべき仕事と遂行した仕事とを管理する機能を携帯電話からの操作を契機に実行するように構成することもできる。この場合は、「DOMINOサーバ R5」の標準的なスケジューラ機能に、アプリケーションプログラムを追加作成することで、それを容易に実現することができる。

【0084】このように、社内メールシステムでは、携帯電話から任意の時点で任意の場所からホストサーバ10が管理している社内情報にアクセスすることができる。アクセスの態様は、上述のように様々であり、あたかもイントラネットLNの内部の固定型端末又はローカルサーバ20のクライアント端末からアクセスしたかの如きである。ホストサーバ10の社内情報は、専用回線網PNを介して接続されたローカルサーバ20のものと共通なので、ローカルサーバ20が属するネットワークに接続されている者との連絡も間接的に行うことができ、グループウェアを効率的に運用することが可能になる。

【0085】なお、このシステムにおいて、受信処理、送信処理、検索処理、予定処理などが実行された場合には、ホストサーバ10から携帯電話へと送信された情報は、送出情報管理部32eにて監視されている。この監視は、例えば、ユーザが閲覧したページのURLを、送出情報管理部32eが抽出することで行われる。送出情報管理部32eは、このような情報の抽出を行うことで、ホストサーバ10から携帯電話にいかなる情報が送出されたか、すなわちユーザがどのページを閲覧したかという情報についての情報である送出情報を生成し、これを送出情報記録部32fへ記録する。この送出情報の記録は、各携帯電話毎に行われ、対応する携帯電話を明らかにしつつ、送出情報記録部32fに記録されている。

【0086】この送出情報は、各携帯電話に課金する際のデータとして利用できる。また、ユーザがホストサーバ10へアクセスする際の労力を軽減すべく、以下のようにも利用できる。すなわち、携帯電話のディスプレイにメニュー画面を表示させるために、送出情報を用いるのである。この場合、アクセスの要求があり、且つアクセス要求をしてきた携帯電話が正規のものと認証された場合に、例えば次のような処理を実行すれば良い。まず、記録されたその送出情報のうちアクセス要求をしてきた携帯電話についての送出情報を、送出情報管理部32eが送出情報記録部32fから読み出して、これを制御部32aへと送る。次いで、これを受け付けた制御部32aがその携帯電話のディスプレイに所定の画像を表示させるためのデータを生成し、これを出入力部31を介して当該携帯電話へと送る。これに基づいて、当該携帯電話のディスプレイに所定のメニュー画像を表示する。表示されるメニュー画像は図28（a）のものと同様の形態とされるが、そこに表示されるメニューは各携帯電話ごとに異なるものとなる。

【0087】<応用例2：アプリケーションのリモート運用システム>本発明のネットワークシステムは、社内メールシステムに代えて、あるいは社内メールシステムとともに、アプリケーションのリモート運用システムとして応用することも可能である。

【0088】この場合の構成は、基本的には社内メールシステムの場合と同様であるが、ローカルサーバ20に、所定のアプリケーションプログラム、例えば共通ファイルではない外部データベースからの情報検索を行う検索プログラム、共通ファイルの中の特定情報を自動的

に印刷する印刷プログラム、社内事務機器の自動制御プログラム等を搭載しておく点、携帯電話の表示部に表示させるウエブメール画面にアプリケーションプログラムの起動用の操作画像をブラウザ画面上に形成しておくか、あるいは専用のコマンド入力を可能にする点が異なる。

【００８９】運用に際しては、携帯電話を所持する者が、例えばブラウザ画面上の操作画像を選択してホストサーバ１０にアクセスする。ホストサーバ１０は、このアクセスに対応するコマンドの内容を解読し、そのコマンドの内容をローカルサーバ２０に通知して該当するアプリケーションプログラムを起動実行させる。ホストサーバ１０は、アプリケーションプログラムが実行された後は、その実行結果の情報をローカルサーバ２０から取得するとともに、取得した情報を携帯電話に通知する。このようにすれば、社内情報の受け渡しだけでなく、外部から社内のアプリケーションプログラムを携帯電話から遠隔起動させることができるので、拡張性に富む社内専用ネットワークシステムを容易に構築できるようになる。

【００９０】なお、この実施形態では、ハウジングを構成するネットワークがイントラネットＬＮであることを前提としたが、ファイアウォールで保護可能なネットワークであればどのような形態のものであっても良い。通常のローカルネットワークでもハウジングを構成することができる。また、好ましい実施の形態として、ファイアウォール１１を通過するのが携帯電話であるものとして説明したが、インターネットＩＮを介した携帯有線端末からのアクセス、すなわち、有線の通信網を介して行われるノートパソコンやＰＤＡからのアクセスであっても、一定条件下でファイアウォール１１を通過させるように構成することが可能である。但し、この場合は、インターネットＩＮに接続された不特定のユーザからのアクセスを許容することになるので、ファイアウォール１１の負担が大きくなる点に留意する必要がある。

【００９１】

【発明の効果】以上の説明から明らかなように、本発明によれば、「なりすまし」を確実に防止できるので、セキュリティ性を確保した専用のグループウェアの実現環境を簡易に構築することができるようになる。

【図面の簡単な説明】

【図１】　本発明が適用されるネットワークシステムの全体構成例を示した図。

【図２】　イントラネットの詳細な構成例を示した図。

【図３】　ルータの構成例を示した図。

【図４】　イントラネットの外側のルータが具備するＮＡＴテーブルの内容説明図であり、（ａ）は公衆通信網からファイアウォールに向かうデータをルーティングする場合の例、（ｂ）はファイアウォールから公衆通信網に向かうデータをルーティングする場合の例を示した図。

【図５】　ＤＯＭＩＮＯサーバを用いたホストサーバの機能構成図。

【図６】　ホストサーバとローカルサーバとの間で実行される複製の仕組みを示した説明図。

【図７】　認証サーバの構成を示す機能ブロック図。

【図８】　認証サーバの情報記録部に記録されたデータを説明するたえの説明図。

【図９】　社内アドレス帳から１０名分程度の個人アドレス帳をコピーする場合の手順説明図。

【図１０】　個人アドレス帳をメールファイルにコピーする場合の手順説明図。

【図１１】　社員がホストサーバにアクセスする場合の手順説明図。

【図１２】　情報アクセス方法の全体的な手順説明図。

【図１３】　認証時に認証サーバで実行される処理の流れを説明するための手順説明図。

【図１４】　受信処理の手順説明図。

【図１５】　受信文処理の手順説明図。

【図１６】　削除処理の手順説明図。

【図１７】　返信処理の手順説明図。

【図１８】　転送処理の手順説明図。

【図１９】　ＦＡＸ処理の手順説明図。

【図２０】　送信処理の手順説明図。

【図２１】　検索処理の手順説明図。

【図２２】　検索リスト表示処理の手順説明図。

【図２３】　新規キーワード処理の手順説明図。

【図２４】　予定処理の手順説明図。

【図２５】　予定リストの新規作成処理の手順説明図。

【図２６】　携帯電話の表示部における表示画面例を示した図で、（ａ）はログイン画面、（ｂ）はメイン画面、（ｃ）及び（ｄ）は受信処理時の画面、（ｅ）は文書表示画面、（ｆ）は送信処理時の画面である。

【図２７】　（ａ）は検索が選択されている様子を示したメイン画面、（ｂ）は検索処理時の画面、（ｃ）は新規キーワードの入力画面、（ｄ）は新規キーワードによる検索結果を表すリスト画面、（ｅ）は検索後の文書表示画面である。

【図２８】（ａ）は予定が選択されている様子を示したメイン画面、（ｂ）は予定リストの一覧表示領域の画面、（ｃ）は予定作成メニューの選択画面、（ｄ）は予定リストの新規作成用のデータ入力画面である。

【符号の説明】

ＬＮ　イントラネット
ＷＮ　無線網
ＭＮ　携帯電話網
ＤＮ　公衆通信網
ＰＮ　専用回線網
ＩＮ　インターネット
Ｔ１　ユーザ端末（携帯電話）

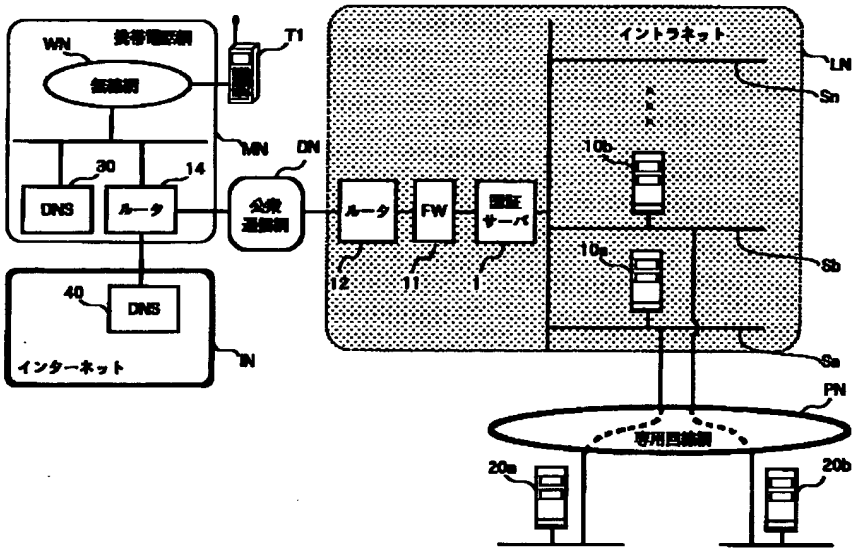
33

Sa～Se　セグメント
10，10a～10e　ホストサーバ
1　認証サーバ
31　出入力部
32　処理部
32a　制御部
32b　プログラム送信部
32c　認証部
32d　情報記録部
32e　送出情報管理部
32e　送出情報記録部
101　CPU

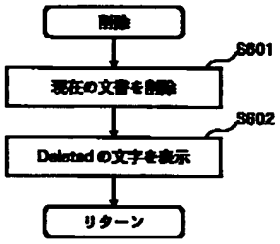
34

102　RAM
103　ROM
104　メールファイル
105　社員データベース
106　文書データベース
107　スケジュールファイル
108　通信アダプタ
11　ファイアウォール
12，13，14　ルータ
10　14　スイッチング・ハブ
20，20a，20b　ローカルサーバ
30，40　DNS

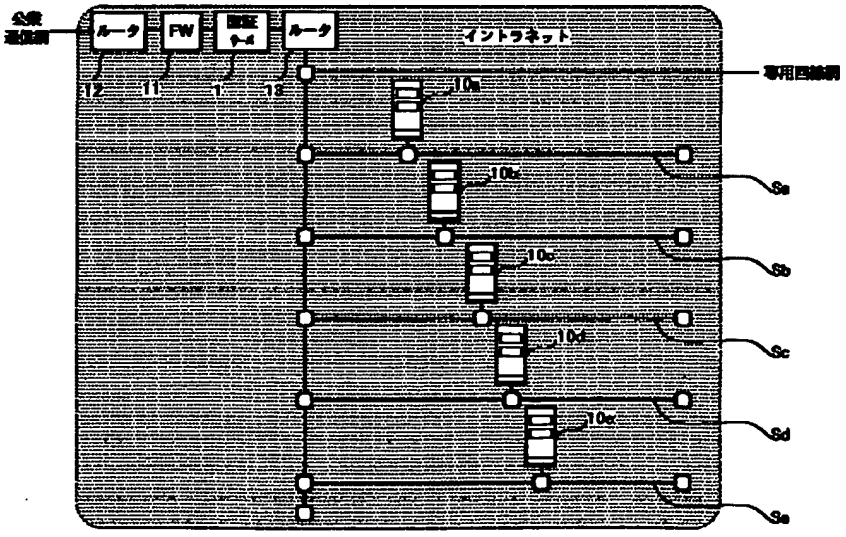
【図1】



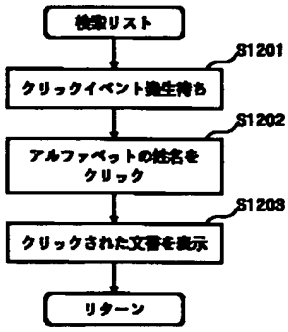
【図16】



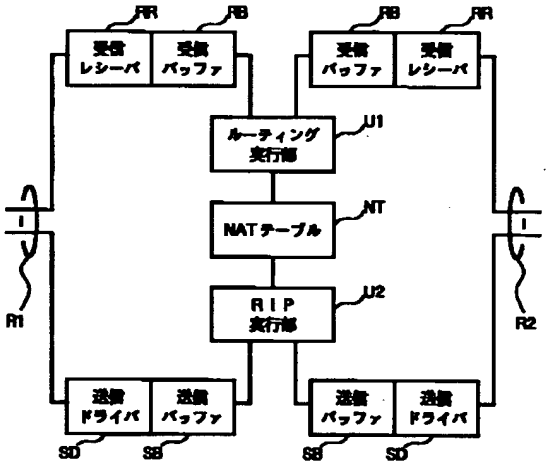
【図2】



【図22】



【図3】



【図4】

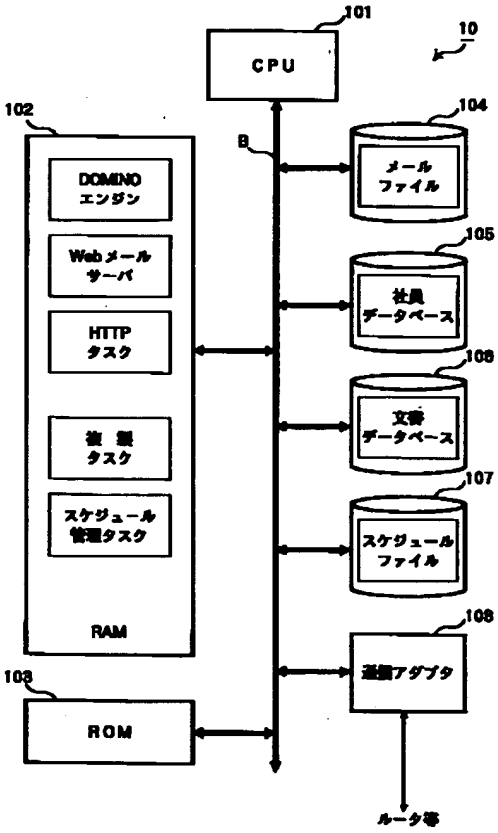
(a)

Destination	Source		
2xx.111.22.33	2xx.444.55.6		
1xx.111.22.33	1xx.444.55.6		

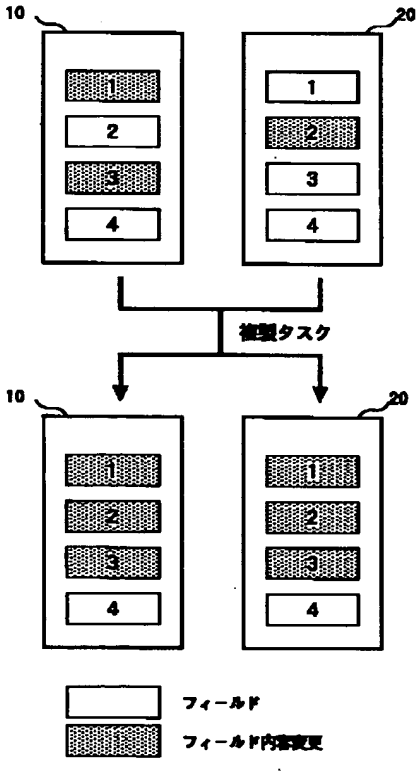
(b)

Destination	Source		
1xx.444.55.6	1xx.111.22.33		
2xx.444.55.6	2xx.111.22.33		

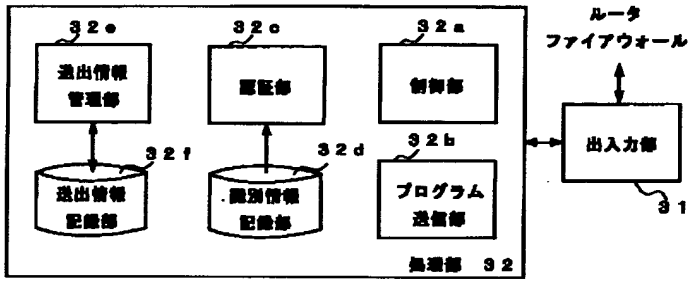
【図5】



【図6】



【図7】



【図8】

個体番号	認証URL	User ID	PASSWORD
00101	1xx. 111. 22. 55	VFDTSK	18STAS8
00102	2xx. 333. 22. 66	eygyoep	54gyrp
00102	2xx. 333. 22. 68	Infoepll	8tfej
03024	1xx. 111. 22. 55	GJYROPS	5DR5GT
：	：	：	：

【図9】

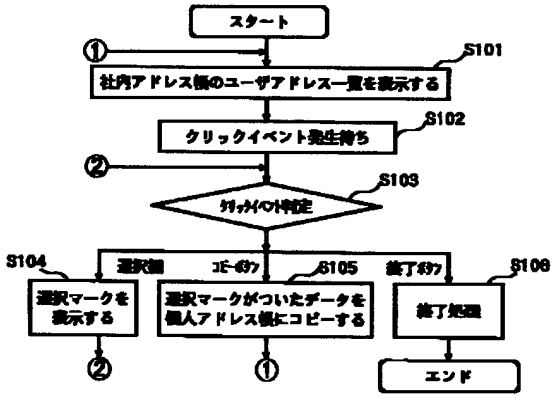
(a)

個体番号	認証ID	認証PSW	停止
00101	AHOL	AOYE	
00102	BHSP	WQAE	1
03024	IUHL	LUYG	

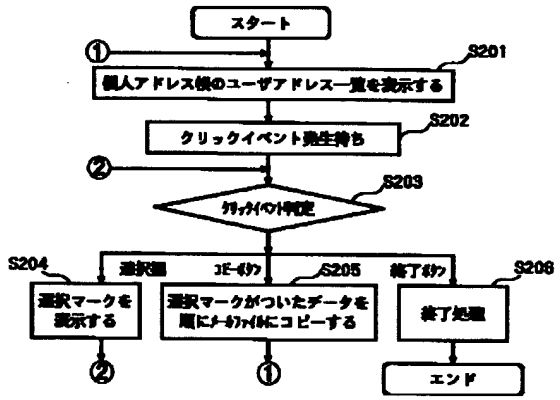
(b)

個体番号	認証URL	UserID	PASSWORD
00101	1xx.111.22.55	VFDTSK	18STAS5
00102	2xx.333.22.66	eygyoep	54gryp
00102	2xx.333.22.68	iufoepll	8tfej
03024	1xx.111.22.55	GJYROPS	5DR5GT

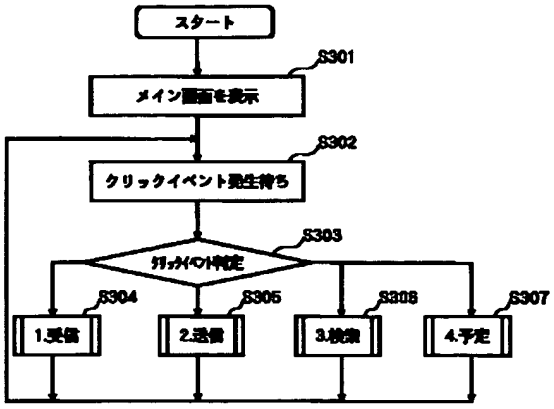
【図10】



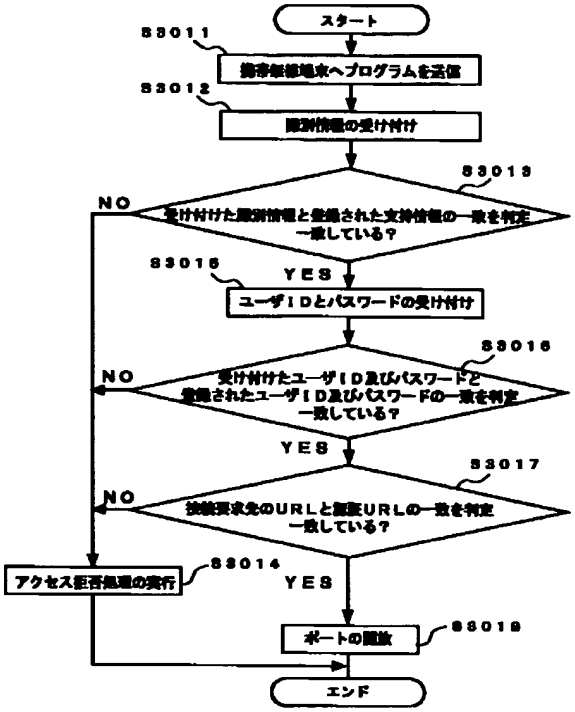
【図11】



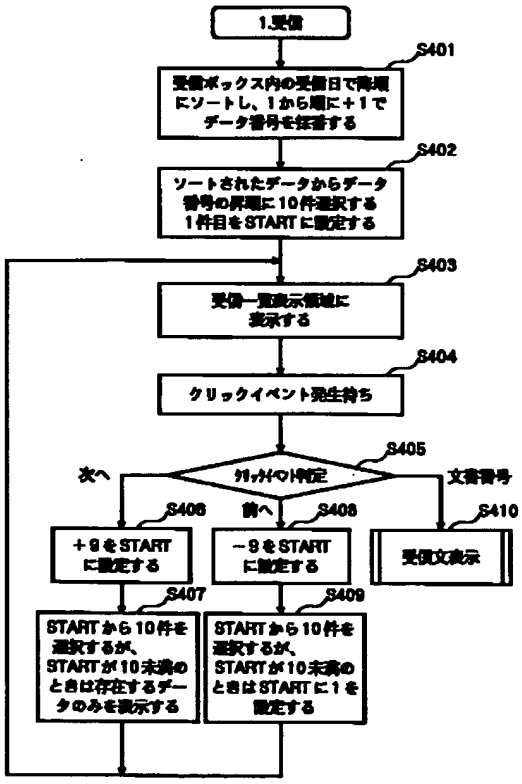
【図12】



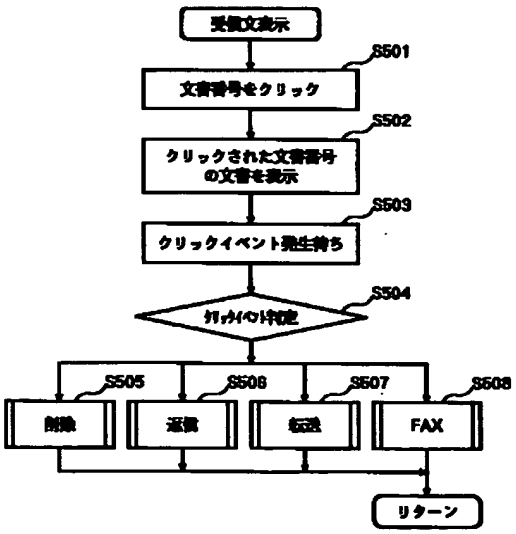
【図13】



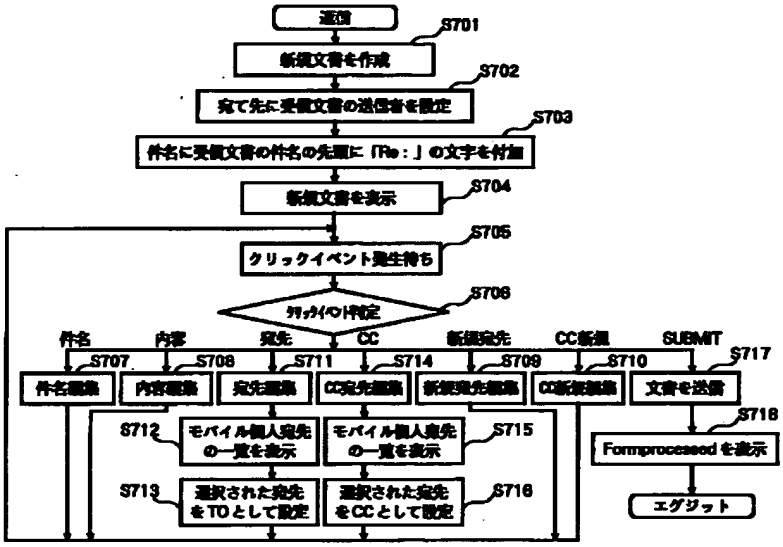
【図14】



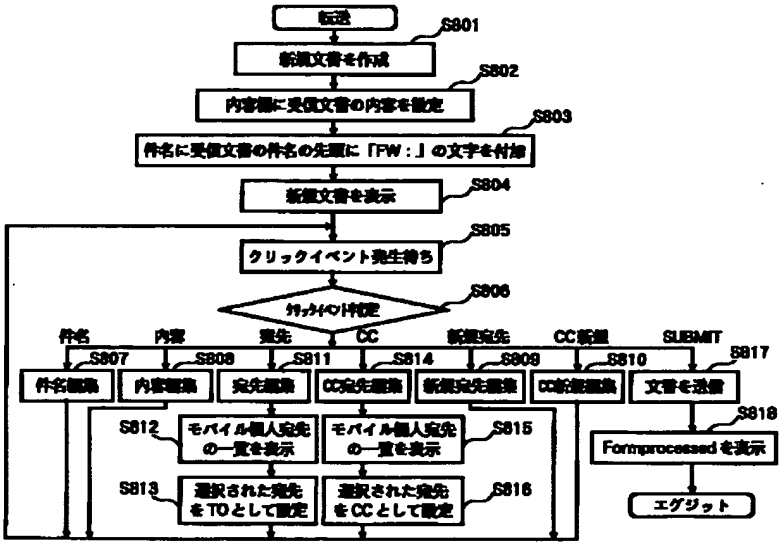
【図15】



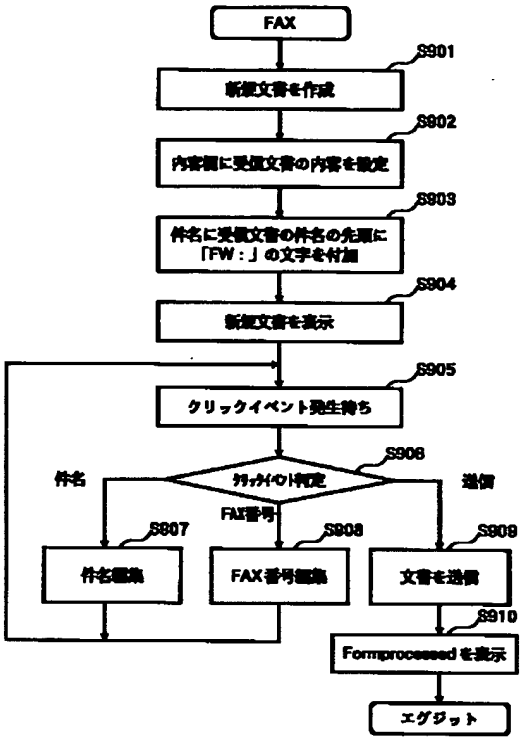
【図17】


返信
S701
転送文書を作成
S702
宛て先に受信文書の送信者を設定
S703
件名に受信文書の件名の先頭に「Re：」の文字を付加
S704
転送文書を表示
S705
クリックイベント発生待ち
S706
クリック判定
件名
内容
宛先
CC
転送宛先
CC転送
SUBMIT
S707
S708
S711
S714
S709
S710
S717
件名編集
内容編集
宛先編集
CC宛先編集
転送宛先編集
CC転送編集
文書を送信
S718
Formprocessedを表示
S712
モバイル個人宛先の一覧を表示
S715
モバイル個人宛先の一覧を表示
S713
選択された宛先をTOとして設定
S716
選択された宛先をCCとして設定
エグジット

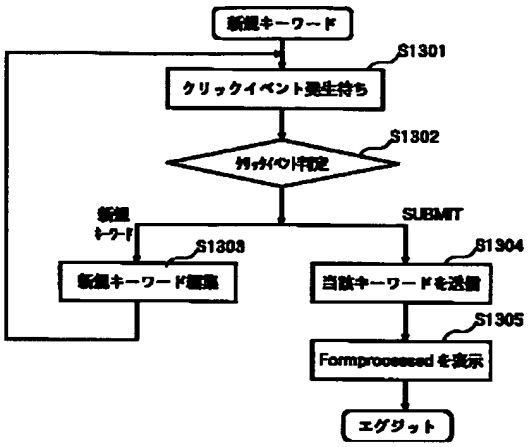
【図18】


転送
S801
転送文書を作成
S802
内容欄に受信文書の内容を設定
S803
件名に受信文書の件名の先頭に「FW：」の文字を付加
S804
転送文書を表示
S805
クリックイベント発生待ち
S806
クリック判定
件名
内容
宛先
CC
転送宛先
CC転送
SUBMIT
S807
S808
S811
S814
S809
S810
S817
件名編集
内容編集
宛先編集
CC宛先編集
転送宛先編集
CC転送編集
文書を送信
S818
Formprocessedを表示
S812
モバイル個人宛先の一覧を表示
S815
モバイル個人宛先の一覧を表示
S813
選択された宛先をTOとして設定
S816
選択された宛先をCCとして設定
エグジット

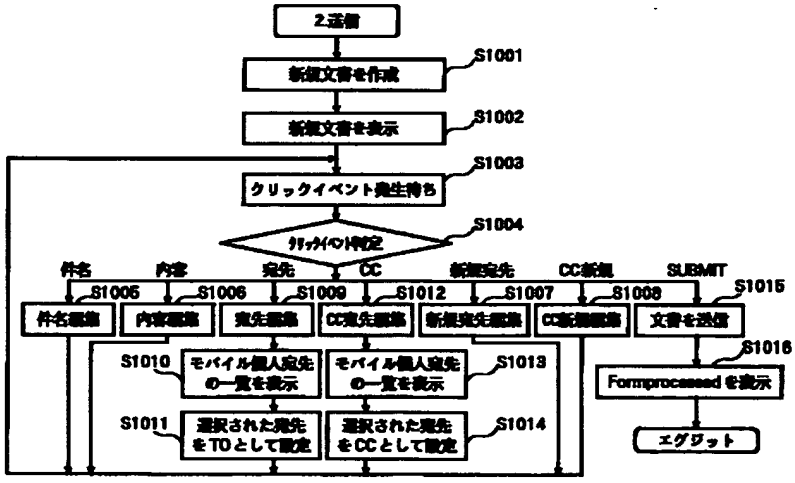
【図19】


FAX
S901
新規文書を作成
S902
内容欄に受信文書の内容を設定
S903
件名に受信文書の件名の先頭に「FW：」の文字を付加
S904
新規文書を表示
S905
クリックイベント発生待ち
S906
クリックイベント判定
件名
FAX番号
送信
S907
件名編集
S908
FAX番号編集
S909
文書を送信
S910
Formprocessed を表示
エグジット

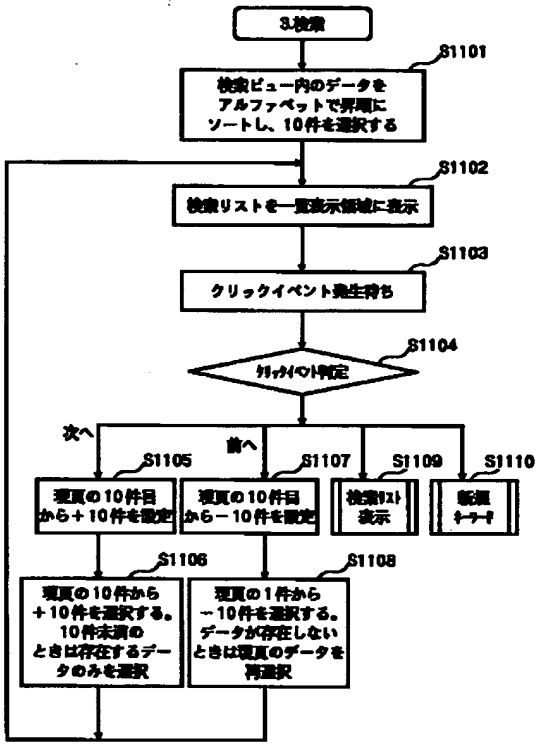
【図23】


新規キーワード
S1301
クリックイベント発生待ち
S1302
クリックイベント判定
新規キーワード
SUBMIT
S1303
新規キーワード編集
S1304
当該キーワードを送信
S1305
Formprocessed を表示
エグジット

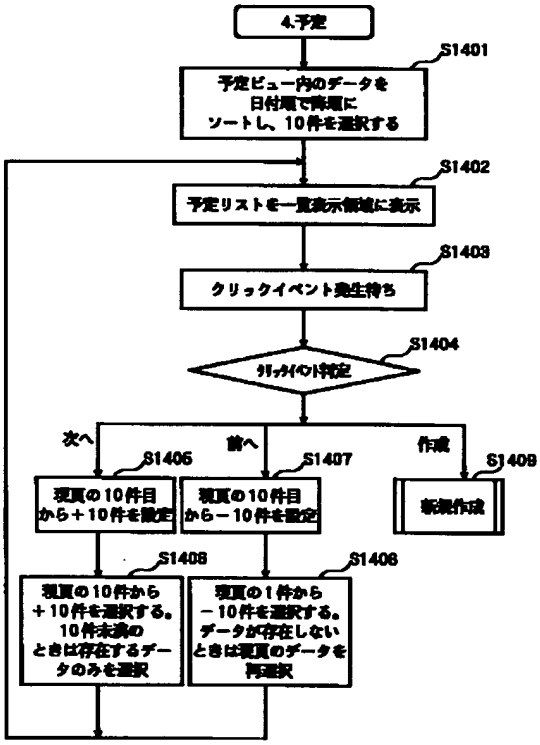
【図20】


2.送信
S1001
新規文書を作成
S1002
新規文書を表示
S1003
クリックイベント発生待ち
S1004
クリックイベント判定
件名
内容
宛先
CC
新規宛先
CC新規
SUBMIT
S1005
S1006
S1009
S1012
S1007
S1008
S1015
件名編集
内容編集
宛先編集
CC宛先編集
新規宛先編集
CC新規編集
文書を送信
S1010
モバイル個人宛先の一覧を表示
S1013
モバイル個人宛先の一覧を表示
S1016
Formprocessed を表示
S1011
選択された宛先をTOとして設定
S1014
選択された宛先をCCとして設定
エグジット

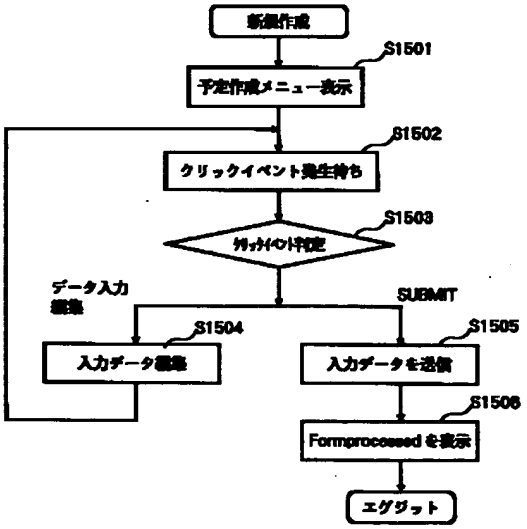
【図21】



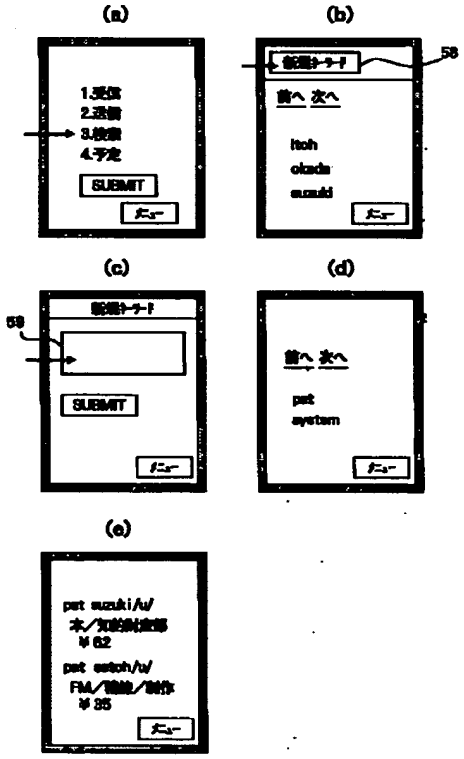
【図24】



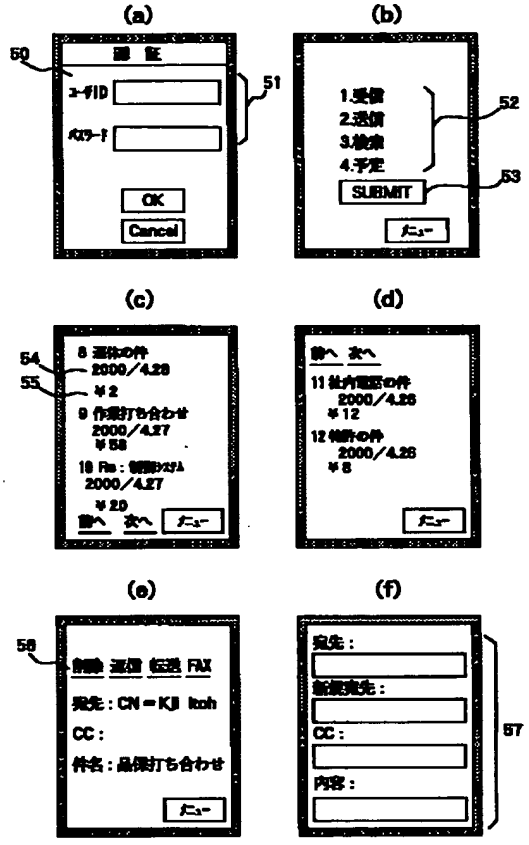
【図25】



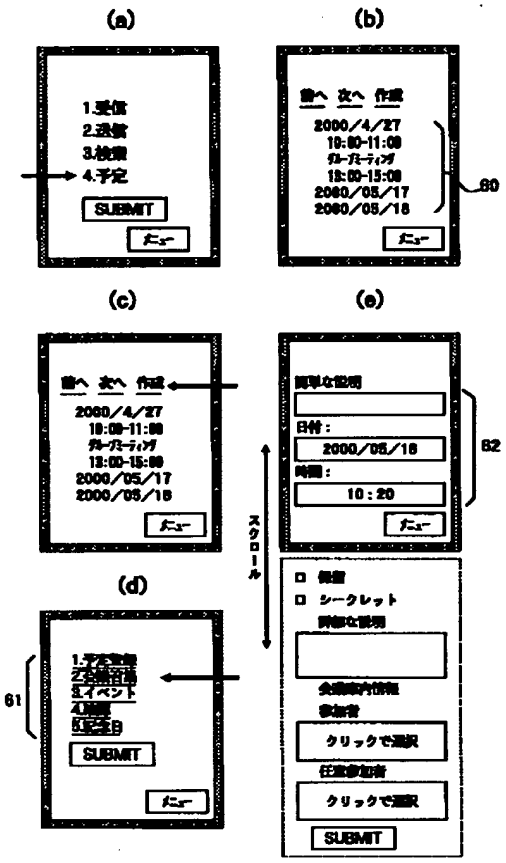
【図27】



【図26】



【図28】



フロントページの続き

Fターム(参考)　5B017 AA07 BA05 CA15
5B085 AE04 BG07
5J104 AA07 AA16 EA03 KA02 KA15
MA01 NA05 PA02 PA07